Criminalité informatique

Leroux, Olivier

Published in:
Les infractions contre les biens

Publication date:
2008

Document Version
le PDF de l'éditeur

CHAPITRE IX

CRIMINALITÉ INFORMATIQUE (1)

Olivier LEROUX
Maître de conférences
aux Facultés Universitaires Notre-Dame de la Paix de Namur
Juge au tribunal de première instance de Bruxelles

Sommaire

(1) L'auteur adresse un amical remerciement à Florence de VILLENFAGNE du Centre de recherches informatique et droit (C.R.I.D.) pour sa relecture attentive et ses observations toujours très judicieuses.

CODE PÉNAL

LIVRE II
DES INFRACTIONS ET DE LEUR RÉPRESSION EN PARTICULIER

TITRE III
Des crimes et des délits contre la foi publique

CHAPITRE IV
[Des faux commis en écritures, en informatique et dans les dépêches télégraphiques]

(ainsi mod. par L. 28 novembre 2000, art. 2)

[Section II*bis*
Faux en informatique

(L. 28 novembre 2000, art. 4)

Art. 210*bis*. §1er. Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§2. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.

§3. La tentative de commettre l'infraction visée au §1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§4. Les peines prévues par les §§1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259*bis*, 314*bis*, 504*quater* ou au titre IX*bis*.]

TITRE IX
Crimes et délits contre les propriétés

CHAPITRE II
Des fraudes

[Section III*bis*
Fraude informatique

(L. 28 novembre 2000, art. 5)

Art. 504*quater*. §1er. [Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal] en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitees ou transmises par un système informatique, ou en modifiant par tout moyen technologique [l'utilisation normale] des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

Ainsi mod. par L. 15 mai 2006, art. 4.

§2. La tentative de commettre l'infraction visée au §1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§3. Les peines prévues par les §§1er et 2 sont doublées si une infraction a l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis* ou au titre IX*bis*.]

[TITRE IX*BIS*
Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes

(L. 28 novembre 2000, art. 6)

Art. 550*bis*. §1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement.

§3. Celui qui se trouve dans une des situations visées aux §§1er et 2 et qui :

1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;

est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six francs belges à cinquante mille francs ou d'une de ces peines seulement.

§4. La tentative de commettre une des infractions visées aux §§1er et 2 est punie des mêmes peines.

§5. [*L. 15 mai 2006, art. 5.* – Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§1er à 4, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.]

§6. Celui qui ordonne la commission d'une des infractions visées aux §§1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent francs à deux cent mille francs ou d'une de ces peines seulement.

§7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§8. Les peines prévues par les §§1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*ter*.

Art. 550*ter*. §1er. [*L. 15 mai 2006, art. 6, 1°.* – Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vint-cinq mille euros ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.]

§2. Celui qui, suite à la commission d'une infraction visée au §1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à septante-cinq mille francs ou d'une de ces peines seulement.

§3. Celui qui, suite à la commission d'une infraction visée au §1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§4. [*L. 15 mai 2006, art. 6, 2°.* – Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.]

§5. Les peines prévues par les §§1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*.

[*L. 15 mai 2006, art. 6, 3°*. – §6. La tentative de commettre l'infraction visée au §1er est punie des mêmes peines.]]

CODE D'INSTRUCTION CRIMINELLE

LIVRE PREMIER
DE LA POLICE JUDICIAIRE ET DES OFFICIERS DE POLICE QUI L'EXERCENT

CHAPITRE VI
Des juges d'instruction

Section II
Fonctions du juge d'instruction

Distinction II
De l'instruction

[§4. Des preuves par écrit, des pièces à conviction et du repérage et de la localisation de télécommunications]

(ainsi mod. par L. 10 juin 1998, art. 4)

Art. 88*quater*. [*L. 28 novembre 2000, art. 9*. – §1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi.

§2. Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et a l'égard des personnes visées à l'article 156.

§3. Celui qui refuse de fournir la collaboration ordonnée aux §§1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

§4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§5. L'État est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système.

(...)

[§6. Des écoutes, de la prise de connaissance et de l'enregistrement de communications et de télécommunications privées

(L. 30 juin 1994, art. 3)

(...)

Art. 90*quater*. (...)

[*L. 28 novembre 2000, art. 12*. – §4. Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

Celui qui refuse de fournir la collaboration ordonnée conformément aux alinéas précédents, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal.]]

Introduction générale

1. Introduction à la criminalité informatique. Comme l'avait rappelé le Professeur Carbonnier, «*l'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquance*» (2). Il n'était dès lors pas surprenant que le développement de l'informatique ait entraîné à sa suite une série de comportements délinquants, le plus souvent motivés par l'appât du gain ou la volonté de nuire (3). Puis, les réseaux se développant et le phénomène allant grandissant, la protection des systèmes informatiques est rapidement devenue un enjeu majeur de l'avenir de l'espace virtuel (4), l'économie, l'administration et la société dans son ensemble dépendant dans une large mesure d'une sécurité informatique efficace (5). Or, de nombreux comportements attentatoires aux systèmes informatiques et aux données qu'ils traitaient restaient impunis, car la matérialité de leur exécution ne correspondait pas aux éléments constitutifs des infractions de droit commun. Ainsi, alors que les informations ou données informatiques étaient, tout autant que les biens matériels, susceptibles d'être atteintes ou dégradées, force était de constater que la législation sanctionnant les atteintes aux biens n'était pas à même d'appréhender suffisamment ce nouveau type de criminalité (6). En cause, notamment, la dématérialisation de l'objet du délit lors d'infractions informatiques qui faisait disparaître l'élément corporel sur la base duquel les poursuites étaient possibles. Le droit pénal étant d'interprétation stricte (7), il nécessitait certaines modifications pour tenir compte des spécificités de la criminalité informatique et ce, afin de respecter le principe constitutionnel «*Nullum crimen sine lege*».

Le besoin d'adopter une législation spécifique apparut clairement dès 1988, lorsque le tribunal correctionnel de Bruxelles eut à connaître de l'affaire *BISTel*, acronyme du système d'information utilisé par le gouvernement (*Belgian Information System by Telephone*). Les faits ayant donné lieu à l'instance étaient relativement simples : deux individus s'étaient introduits de façon illicite, au moyen d'un mot de passe détourné, dans le serveur informatique assurant notamment la communication électronique entre les cabinets ministériels. Ils avaient été condamnés pour cela du chef de faux et usage de faux (pour avoir introduit un mot de passe consistant en un code électronique attribué au premier ministre), vol qualifié (vol avec fausses clés d'énergie électrique) et interception illégale de télécommunications (8). Mais sur l'appel des prévenus, la Cour avait réformé le jugement et écarté les trois premières préventions pour ne retenir que la quatrième (9). Cet arrêt avait mis en

(2) J. CARBONNIER, *Sociologie Juridique*, Paris, P.U.F., 1978, p. 401.

(3) Alors qu'il est considéré par beaucoup que le premier ordinateur a été créé en 1946 (soit l'ENIAC, élaboré par I.B.M.), on recense déjà un premier délit informatique en 1966, année durant laquelle les fichiers de comptes d'une banque de Minneapolis avaient été altérés.

(4) Voy. not. à ce propos, le rapport annuel du CERT, *State of the Practice of Intrusion Detection Technologies*, www.cert.org.

(5) U. SIEBER, «Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique», *R.I.D.P.*, 1993, vol. 64, p. 53.

(6) Même si, comme le souligne U. SIEBER, l'évolution d'une société industrielle vers une société postindustrielle et le changement de paradigme des objets corporels en objets incorporels avaient atteint le droit pénal et que se dessinait depuis les années 1970 l'ébauche d'un droit pénal de l'information (notamment à l'égard de la protection de la vie privée d'abord, de la lutte contre la délinquance économique ensuite, de la sauvegarde de la propriété intellectuelle enfin) (U. SIEBER, «Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique», *op. cit.*, p. 55).

(7) Sous réserve de l'interprétation dite technologique ou téléologique admise par la Cour de cassation selon laquelle «il est permis au juge statuant en matière répressive d'appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de prévoir à l'époque de la promulgation de la disposition pénale, à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de l'infraction» (Cass., 4 mai 1988, *Pas.*, 1988, I, p. 1071; Cass., 11 septembre 1990, *Pas.*, 1990, I, p. 36).

(8) Le tribunal avait considéré que «se procurer irrégulièrement un accès à un système informatique ne constitue pas en soi un délit sanctionné pénalement en vertu du droit belge. Une telle procédure constitue toutefois un faux en écritures par abus de mot de passe, vol et détournement d'une communication confiée à la R.T.T. [...]. La notion d'écrit ne se limite pas aux modes d'écriture que le législateur connaissait lors de l'élaboration du Code pénal. Peuvent constituer un écrit, un code ou un mot de passe introduits dans un ordinateur». On notera que les prévenus étaient également poursuivis du chef de destruction de bâtiments, œuvres ou constructions (en l'occurrence la destruction du système électronique de communication), mais cette prévention n'a pas été retenue par le tribunal (Corr. Bruxelles, 8 novembre 1990, *Computerr.*, 1991, p. 31, note A. MEIJBOOM; *D.I.T.*, 1991/1, p. 51, note C. ERKELENS; *J.T.*, 1991, p. 11, note; B. de SCHUTTER, «Het Belgisch Bistel-syndroom», *Computerr.*, 1991, pp. 164-166).

(9) Bruxelles, 24 juin 1991, *Rev. dr. pén.*, 1992, p. 340. Concernant la prévention de vol qualifié, la Cour avait estimé qu'il n'y avait pas eu intention de soustraire une «chose» appartenant à autrui, de sorte que l'élément intentionnel requis pour le vol n'était pas établi. Concernant la prévention de faux, la Cour avait considéré qu'elle ne pouvait mener à une condamnation en l'espèce car : «le mot de passe constituant dans un code électronique utilisé par les prévenus ne constitue pas une écriture, et plus précisément, ne constitue pas un signe graphique au sens des articles 193 et suivants du Code pénal». Reprenant la définition de l'écriture telle que développée par la Cour de cassation, la Cour d'appel de Bruxelles avait décidé que «l'écriture», au sens des art. 193 et s. du C. pén., devait être entendue comme un ensemble de signes graphiques «qui figurent sur un support matériel, pour constater un acte ou un fait juridique et que le public peut considérer comme vrai». En d'autres termes, la Cour avait considéré que l'écriture dont il était question devait être la matérialisation d'une pensée dans un système de signes qui pouvaient être lus et compris, ce qui n'était très certainement pas le cas de données informatiques introduites ou stockées dans un système, lesquelles ne constituent pas des signes graphiques intelligibles par eux-mêmes.

LARCIER

évidence les insuffisances et les manquements du système pénal face aux nouvelles technologies. La nécessité d'adapter le Code pénal et le Code d'instruction criminelle aux défis de la criminalité informatique ne pouvait plus être ignorée par le législateur (10).

2. Définition, classification et caractéristiques. Pendant longtemps, la criminalité informatique (ou cybercriminalité) n'a pas été légalement définie. Elle englobait de façon générale, selon l'ébauche de définition qu'en avait donnée l'O.C.D.E. : «*tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transmission de données*» (11). La délinquance informatique était donc celle dont la réalisation impliquait, directement ou indirectement, l'usage d'un système informatique (12).

La doctrine a traditionnellement distingué la criminalité informatique spécifique de la criminalité informatique aspécifique (13).

3. Criminalité informatique spécifique. La criminalité informatique spécifique recouvre les infractions ayant l'informatique pour cible et vise donc les comportements dirigés contre un système informatique ou les données qu'il contient. L'expression la plus évidente de ce type de criminalité consiste en l'accès non autorisé à un système informatique (également appelé *hacking*), dans le sabotage de données informatiques (en ce compris l'entrave au fonctionnement d'un système informatique) ou dans la fraude informatique.

(10) Avant l'adoption d'une loi spécifique, différents juges avaient eu à connaître d'affaires relevant, à des degrés divers, de la criminalité informatique et avaient appliqué, de façon plus ou moins convaincante, des dispositions tirées du Code pénal ou de lois particulières. Parmi celles-ci, on relève notamment la loi du 8 août 1983 organisant un registre national des personnes physiques, la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, la loi du 30 juin 1994 relative aux droits d'auteur et aux droits voisins, la loi du 30 juin 1994 relative à la protection juridique des programmes d'ordinateur, la loi du 30 juin 1994 relative aux écoutes téléphoniques, la prise de connaissance et l'enregistrement de communications et télécommunications privées et la loi du 10 août 1998 sur la protection des bases de données (voy. not. O. VANDEMEULEBROEKE, «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)», in *Internet sous le regard du droit*, Bruxelles, éd. Jeune Barreau, 1997, p. 155; J.-P. SPREUTELS, «Les crimes informatiques et autres crimes dans le domaine de la technologie informatique en Belgique», in *Information Technology Crime – National Legislations et International Initiatives* (U. SIEBER ed.), coll. Ius Informationis, vol. 6, Köln, Carl Heymanns Verlag KG, pp. 49-65).

(11) O.C.D.E., *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris, 1986, p. 7. Pour d'autres définitions et leur analyse, voy. R. KASPERSEN, *Strafbaarstelling van computermisbreuk*, Rotterdam, Kluwer, 1990, pp. 29 et s.

(12) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique», in *Actualités du droit des technologies de l'information et de la communication*, CUP, vol. 45, Liège, éd. Formation permanente CUP, février 2001, p. 45.

(13) Sur cette distinction, voy. not. U. SIEBER, *Legal Aspects of Computer-related Crime in the Information Society*, COM-CRIME Study, Rapport pour la Commission européenne, 1er janvier 1998.

4. La criminalité informatique aspécifique. La criminalité informatique aspécifique englobe les infractions pour la réalisation desquelles l'informatique n'est utilisée que comme outil. Ces infractions consistent le plus souvent en une adaptation technologique d'infractions préexistantes en droit commun. Cette seconde catégorie appréhende donc l'outil informatique en tant qu'instrument de réalisation d'infractions pour l'accomplissement desquelles le recours à l'informatique n'est pas indispensable (14). Il s'agit notamment de la diffusion, par des réseaux informatiques, d'images pédophiles, d'injures ou de propos racistes ou révisionnistes, mais aussi de la réalisation d'infractions de harcèlement, de diffamation, de blanchiment ...

Cette distinction générale a été largement reprise depuis (15).

Qu'elle soit spécifique ou aspécifique, la criminalité informatique se caractérise par la dématérialisation de son objet ou de ses moyens, sa dimension souvent internationale, le relatif anonymat dont ses auteurs peuvent bénéficier (ou croient pouvoir bénéficier) et son caractère multiforme (atteintes à la vie privée, espionnage, sabotage, piratage, incitations à la haine ou au racisme, pédophilie, fraude, escroquerie, voire même cyber-terrorisme (16) ...).

(14) En doctrine, la distinction a encore été faite, au sein de cette seconde catégorie, entre les infractions consistant en des «actes où l'informatique a un caractère incident au délit», c'est-à-dire les infractions réalisées par la voie informatique sans que l'informatique soit nécessaire pour les commettre mais pour lesquelles elle permet d'agir plus vite, plus facilement, autrement, et celles consistant en de «nouvelles versions de délits traditionnels», soit les infractions classiques réalisées par la voie informatique (David L. CARTER, «Computer Crime Categories : How Techno-criminals operate», *FBI Law Enforcement Bulletin*, 1992, http://nsi.org/library/Compsec/crimecom.html).

(15) Voy. not. D. BAINBRIDGE, *Introduction to computer law*, London, Longman, 2000, p. 291; G. CHAMPY, *La fraude informatique*, Presses Universitaires d'Aix-Marseille, 1992, pp. 53 et s.; S. CHARNEY, «Computer Crime. Law Enforcement's Shift from a Corporeal Environment to an Intangible, Electronic World of Cyberspace», *Federal Bar News & Journal*, 1994, n° 7, p. 489; B. DEJEMEPPE, «Le parquet face à la criminalité informatique : entre droit et non-droit», *Journ. proc.*, 1993, n° 239, p. 12; M.D. GOODMAN, «Why the police don't care about computer crime», *Harvard Journal of Law & Technology*, 1997, n° 3, p. 468; D.B. PARKER, *Fighting Computer Crime*, New-York, éd. Wiley, 1998, p. 16; A. VAN BAVEL, «De strafrechtelijke aansprakelijkheid van de aanbieders van netwerkdiensten», *A. & M.*, 1998, pp. 336 et s.; O. VANDEMEULEBROEKE, «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)», *op. cit.*; P. VAN EECKE, *Criminaliteit in cyberspace*, Gand, Mys & Breesch, 1997, p. 15.

(16) Ce dernier vocable, souvent repris dans la littérature de sécurité informatique, est imprécis et dénué de valeur juridique. Il recouvre de façon incertaine toutes formes de criminalité informatique impliquant des structures vitales et donc susceptibles d'entraîner la mort d'êtres humains (notamment en cas d'attaques de systèmes informatiques utilisés pour la gestion du partage de l'espace aérien ou la distribution de médicaments). Voy. not. à ce propos, A. O'DAY, *Cyberterrorism*, Hants, The International Library of Essays in Terrorism, 2004, 312 p. Cette forme de criminalité avait été envisagée par le législateur, puisque les travaux préparatoires de la loi du 28 novembre 2000 citent l'hypothèse de la manipulation frauduleuse de données relatives au dosage pour l'administration de médicaments et susceptibles de provoquer le décès de patients (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 2013/001, p. 4).

5. Dispositions applicables en droit interne. En droit interne, la criminalité informatique est essentiellement appréhendée par la loi du 28 novembre 2000 relative à la criminalité informatique (17) (18) (19).

Cette loi, entrée en vigueur le 13 février 2001, se compose de deux volets distincts (20).

(17) L. 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, p. 2909.

(18) Sur la criminalité informatique en droit belge avant l'adoption de la loi du 28 novembre 2000, voy. not. G.L. BALLON, «Het bewijs en de moderne technieken», *Computerr.*, 1991, p. 14; J.-P. BUYLE et O. POELMANS, «Internet, quelques aspects juridiques», *D.I.T.*, 1996/4, pp. 6 et s.; I. COLLARD, «Criminalité informatique en Belgique : hier, les ténèbres. Demain ...», *Rev. Ubiquité*, 1998, n° 1, p. 73; M. DE JAEGER, «Enkele beschouwingen over computerfraude en strafrecht», *Acc. Bedr.*, 1987, pp. 129 et s.; B. DEJEMEPPE, «Le parquet face à la criminalité informatique : entre droit et non-droit», *op. cit.*; B. de SCHUTTER, «Computerfraude», *Inleiding tot het computergebruik en zijn toepassingsproblemen in het recht*, Antwerpen, Kluwer, 1985, pp. 51 et s.; B. de SCHUTTER, «La criminalité liée à l'informatique», *Rev. dr. pén.*, 1985, pp. 383 et s.; B. de SCHUTTER (éd.), *Informaticacriminaliteit*, Antwerpen, Kluwer rechtswetenschappen, 1988, pp. 141 et s.; B. de SCHUTTER, «Het Belgisch Bistel-syndroom», *op. cit.*; B. de SCHUTTER et B. SPRUYT, «Computerfraude, de relatieve onmacht van het interne en het internationale strafrecht», *Technologie en recht*, Antwerpen, Kluwer rechtswetenschappen, 1987, pp. 353 et s.; C. ERKELENS, «Beteugeling van computercriminaliteit», *Panopticon*, 1985, pp. 334 et s.; C. ERKELENS, «La délinquance informatique belge et le droit pénal belge», *Dr. inform.*, 1985/6, p. 21; Ph. GÉRARD et V. WILLEMS, «Prévention et répression de la criminalité sur internet», in *Internet face au droit* (E. MONTERO éd.), Cahiers du CRID, n° 12, Diegem /Namur, Story-Scientia/C.R.I.D., 1997, pp. 144 et s.; M. JAEGER, «La fraude informatique», *Rev. dr. pén.*, 1985, p. 347; P. GLINEUR, *Droit et éthique de l'informatique*, Bruxelles, éd. Story-Scientia, 1991, pp. 179 et s.; S. GUTWIRTH, «De beteugeling van informaticafraude. Naar een nieuw 'informaticarecht'», *R.W.*, 1985-1986, col. 2459 et s.; P. HELSEN, «Diefstal van computergegevens», *Jura Falc.*, 1997-1998, pp. 261 et s.; O.C.D.E., *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris, 1986, p. 7; J. PRADEL et C. FEUILLARD, «Les infractions commises au moyen de l'ordinateur», *Rev. dr. pén.*, 1985, p. 311; J.-P. SPREUTELS, «La responsabilité pénale découlant des atteintes aux applications de l'informatique», in *Informatique et droit en Europe*, Bruxelles, éd. ULB/Bruylant, 1984, pp. 277 et s.; J.-P. SPREUTELS, «Le vol de données informatiques», *Rev. dr. pén.*, 1991, p. 1027; J.-P. SPREUTELS, «Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Belgique», *R.I.D.P.*, 1993, p. 161; B. SPRUYT, «Computers op de strafbank. Analyse van het fenomeen informaticacriminaliteit : nationale en internationale strafrechtelijke perspectieven», in *Informaticacriminaliteit*, Antwerpen, Kluwer rechtswetenschappen, 1988, pp. 321-326; O. VANDEMEULEBROEKE, «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)», *op. cit.*; M.C.R. VAN DER NET, «*Locus delicti* op het internet», *Computerr.*, 1996, pp. 390 et s.; C. VANDENBERGHE, «Diefstal van computergegevens. Revolutie in het strafrecht», *Computerr.*, 1986, pp. 44 et s.; D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à internet», *Internet sous le regard du droit*, Bruxelles, éd. Jeune Barreau, 1997, pp. 291 et s.; P. VAN EECKE, *Criminaliteit in cyberspace : misdrijven, hun opsporing en vervolging op de informatiesnelweg*, Gent, Mys & Breesch, 1997, 121 p.; I. VAN MOLLE, «Computerfraude», *Kijk uit*, Leuven, éd. S.B.B., 1999, pp. 81 et s.; R. VERSTRAETEN, «Diefstal van computergegevens», *R.W.*, 1985-1986, col. 216; E. WÉRY, «Internet hors la loi?», *J.T.*, 1997, p. 417; V. WILLEMS, «Belgique : où en est-on en matière de criminalité informatique?», *D.I.T.*, 1994/1, pp. 70 et s.

(19) On relèvera encore la loi du 12 mai 2003 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel relatifs aux services de la société de l'information, *M.B.*, 26 mai 2003.

(20) Pour des commentaires doctrinaux de la loi du 28 novembre 2000, voy. not. : P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht : een wet die te laat komt of een wet die er nooit had moeten komen?», *T. Strafr.*, 2001, pp. 286 et s.; P. DE HERT et G. LICHTENSTEIN, «De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht», *CBR Jaarboek 2002-2003*, Anvers, Maklu, 2003, pp. 345-420; F. de VILLENFAGNE et S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A.&M.*, 2001, pp. 60-81; www.droit-technologie.org; J. DUMORTIER, B. VAN OUDENHOVE et P. VAN EECKE, «La nouvelle législation belge

Le premier introduit dans l'ordre législatif de nouvelles incriminations propres à la criminalité informatique. L'objectif de la loi était en effet, d'une part, d'adapter les incriminations existantes au regard des nouveaux moyens de les commettre et, d'autre part, d'incriminer les comportements nouveaux visant à porter atteinte à l'intégrité, la sécurité et la confidentialité des systèmes d'information. La loi insère ainsi dans le Code pénal les articles 210*bis*, relatif au faux informatique et à l'usage de faux informatique, 504*quater*, relatif à la fraude informatique, 550*bis*, relatif à l'accès non autorisé dans un système informatique et aux infractions voisines, et 550*ter*, relatif au sabotage informatique.

Le second volet de la loi s'attache à aménager certaines dispositions de procédure pénale en vue d'assurer la collecte de preuves électroniques. La loi modernise ainsi le Code d'instruction criminelle en ce qui concerne notamment les saisies et les recherches informatiques, mais également la loi du 21 mars 1991 relative aux entreprises publiques économiques en ce qui concerne le repérage et l'identification (21).

Depuis son entrée en vigueur, la loi du 28 novembre 2000 a été modifiée par la loi du 15 mai 2006 suite à la signature par la Belgique, le 23 novembre 2001, de la Convention cybercriminalité du Conseil de

relative à la criminalité informatique», *Vigiles*, 2001, pp. 44-62; S. EVRARD, «La loi du 28 novembre 2000 relative à la criminalité informatique», *J.T.*, 2001, pp. 241 et s.; H. HAELTERMAN et G. LICHTENSTEIN, «Informaticacriminaliteit en de wet van 28 november 2000», *Private veiligheid*, n° 7/2001, p. 14; T. LAUREYS, *Informatica criminaliteit*, Gand, Mys & Breesch, 2001, 117 p.; B. MAGREZ, «Analyse de l'avant-projet de loi belge portant sur la criminalité informatique», www.juriscom.net/pro/1/crim19980901.htm; C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *Rev. dr. pén.*, 2001, pp. 611 et s.; J. STEENLANT, «Criminalité informatique – vers une répression pénale efficace?», *Bull. FEB*, 2000, pp. 18 et 54; E. ROGER FRANCE, «La criminalité informatique», *Actualités de droit pénal*, Bruxelles, Bruylant, 2005, pp. 101-133; E. ROGER FRANCE, «Transactions électroniques et criminalité informatique : quelle répression?», in *Aspects juridiques du paiement électronique. Volume 2*, Malines, Kluwer, 2004, pp. 229-257; P. VAN EECKE, «Het voorontwerp van wet inzake informaticacriminaliteit», in *Recente ontwikkelingen in informatica et telecommunicatierecht* (J. DUMORTIER dir.), Brugge, die Keure, 1999, pp. 219 et s.; Th. VERBIEST et E. WÉRY, *Le droit de l'internet et de la société de l'information. Droits européen, belge et français*, Bruxelles, Larcier, 2001.

(21) Signalons encore que l'A.R. du 9 janvier 2003 portant exécution des articles 46*bis*, §2, alinéa 1er, 88*bis*, §2, alinéas 1er et 3, et 90*quater*, §2, alinéa 3, du Code d'instruction criminelle ainsi que de l'article 109*ter*, E, §2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (*M.B.*, 10 février 2003, p. 6614), précisant les données d'identification devant être collectées par les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications dans le cadre de leur collaboration avec les autorités judiciaires, ne s'applique pas aux fournisseurs d'accès à l'internet. Ceux-ci demeurent soumis aux dispositions générales de la loi du 28 novembre 2000 (et sont donc toujours obligés de prêter leur concours), même si les modalités techniques de ce concours ne sont pas fixées. À l'heure actuelle, et dans l'attente d'un arrêté royal précisant la liste des données techniques devant être collectées, il leur revient de déterminer eux-mêmes ces données, ce qui n'est pas sans créer une incertitude juridique. Le Conseil d'État avait critiqué la différence de traitement qui était faite entre les fournisseurs de services Internet et les autres opérateurs et fournisseurs de services de télécommunications (Avis n° 33.354/4 du 2 mai 2002, Rapport au Roi de l'A.R. du 9 janvier 2003), mais le gouvernement a estimé que cette différence était fondée sur un motif objectif et raisonnable, à savoir la spécificité du secteur Internet.

l'Europe (22) et de son Protocole additionnel relatif à l'incrimination d'acte de nature raciste et xénophobe commis par le biais de systèmes informatiques (23), en vue de mettre le texte belge en conformité avec cette Convention (24) (voy. *infra*).

Enfin, en marge de la loi du 28 novembre 2000, la loi du 11 mars 2003 relative à certains aspects juridiques de la société de l'information (25) transpose en droit interne la directive européenne dite «commerce électronique» du 8 juin 2000 (26). Cette loi met en place un cadre juridique pour les services en ligne et le commerce électronique sur l'internet et règle, entre autres choses, la responsabilité tant civile que pénale des prestataires intermédiaires d'internet (à savoir, notamment, des hébergeurs et des fournisseurs d'accès). La loi consacre un compromis (inspiré du droit américain) en instituant une exemption totale de responsabilité sous conditions au profit des activités de transmission des informations sur un réseau de communications et de fourniture d'accès à un tel réseau, ainsi qu'une exonération partielle de responsabilité au profit des activités d'hébergement et de stockage sous forme de cache des informations à la demande d'un destinataire du service (27). L'approche de la loi est horizontale en ce qu'elle vise à

(22) Ci-après dénommée «la Convention».

(23) *Cf. infra*.

(24) L. 15 mai 2006 modifiant les articles 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal, *M.B.*, 12 septembre 2006. Voy., à propos de cette loi, B. DOCQUIR, «Loi du 15 mai 2006 : nouvelles définitions des infractions en matière de criminalité informatique», *R.D.T.I.*, 2006, n° 26, pp. 287-294.

(25) L. 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003, p. 12963. Pour une étude de la loi, voy. E. MONTERO, M. DEMOULIN et C. LAZARO, «La loi du 11 mars 2003 sur les services de la société de l'information», *J.T.*, 2004, pp. 81 et s. Voy. égal. Th. VERBIEST et E. WÉRY, «La responsabilité des fournisseurs d'outils de recherche et d'hyperliens», *Légipresse*, n° 181, 2001, pp. 49-53.

(26) Dir. 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive commerce électronique»), *J.O.C.E.*, L 178 du 17 juillet 2000, p. 1. A. STROWEL, N. IDE et F. VERHOESTRAETE, «La directive du 8 juin 2000 sur le commerce électronique : un cadre juridique pour l'internet», *J.T.*, 2001, pp. 133-145.

(27) Sur la responsabilité des prestataires intermédiaires, voy. not. : A. LUCAS, «La responsabilité des fournisseurs de services internet : derniers développements jurisprudentiels», *J.T.*, 2001, pp. 165-172; H. HIJMANS, «Aansprakelijkheid op het internet na de totstandkoming van richtlijn 2000/31/EG», *Computerr.*, 2000, pp. 234-239; A. STROWEL et N. IDE, «La responsabilité des intermédiaires sur internet», *R.I.D.A.*, 3/2000, pp. 3-167; E. MONTERO, «La responsabilité des prestataires intermédiaires sur les réseaux», in *Le commerce électronique européen sur les rails? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du C.R.I.D., n° 19, Bruxelles, Bruylant, 2001, pp. 289 et s.; Th. VERBIEST et E. WÉRY, «La responsabilité des fournisseurs de services internet : derniers développements jurisprudentiels», *J.T.*, 2001, pp. 165-172; J.-Ph. HUGOT, «De nouvelles responsabilités sur l'internet : du vide au flou juridique», *Légipresse*, 2002, n° 191-II, pp. 51-55; Liège, 28 novembre 2001, *J.L.M.B.*, 2004, p. 762; *J.T.*, 2002, p. 308, note A. CRUQUENAIRE et J. HERVEG, «La responsabilité des intermédiaires de l'internet et les procédures en référé ou comme en référé»; *R.D.J.P.*, 2002, p. 261.

s'appliquer tant en matière d'atteinte aux droits d'auteurs ou aux droits voisins qu'en cas de commission d'une infraction de droit commun. On notera toutefois que les exonérations de responsabilité ne couvrent que certaines activités bien déterminées (à savoir le transport, la fourniture d'accès à un réseau, le stockage temporaire sous forme de cache et l'hébergement) (28) et ne recouvrent donc pas les activités d'édition et de production de contenus ni la fourniture de liens hypertextes ou de services d'annuaires ou de moteurs de recherche (29). Ces activités relèvent du droit commun de la responsabilité (30).

On notera encore que la loi du 28 novembre 2000 ne modifie en rien les règles de détermination de la compétence territoriale (31). Conformément au principe *locus delicti commissi* consacré à l'article 3 du Code pénal, le système de la territorialité attribue compétence aux juridictions et à la loi du lieu où se commet l'infraction, quelle que soit la nationalité de l'auteur ou de la victime ou la gravité de l'infraction (32). Il faut donc, mais il suffit, pour qu'une infraction informatique puisse être poursuivie en Belgique, qu'un élément constitutif ou aggravant de cette infraction ait été réalisé sur le territoire belge ou s'y soit matérialisé (33). En tant que

(28) Cass., 3 février 2004, *Pas.*, 2004, p. 200; *A. & M.*, 2005, p. 259 (somm.), note; *Computerr.*, 2004, p. 242, note S. DE SCHRIJVER; *Juristenkrant*, 2004, n° 85, p. 6; *R.D.T.I.*, 2004, n° 19, pp. 51-59, note F. de PATOUL et I VEREECKEN, «La responsabilité des intermédiaires de l'internet : première application de la loi belge». La Cour de cassation a estimé en l'espèce que le régime d'exonération de responsabilité établi par cette loi entraînait une exemption de peine et devait donc avoir un effet rétroactif. Mais elle a également considéré qu'en l'absence de définition, l'intermédiaire était celui dont «l'activité revêt un caractère purement technique, automatique et passif, ce qui implique que l'intermédiaire ne connaît pas et n'exerce pas de contrôle sur l'information qui est transmise et stockée».

(29) Comme le soulignent E. MONTERO, M. DEMOULIN et C. LAZARO («La loi du 11 mars 2003 sur les services de la société de l'information», *op. cit.*, p. 92), ce point n'est précisé ni dans les articles, ni dans les considérants de la directive, mais on trouve diverses indications en ce sens dans le commentaire article par article de la proposition de directive. Sur la responsabilité en matière d'hyperliens, voy. A. STROWEL et N. IDE, «La responsabilité des intermédiaires sur internet : actualités et question des hyperliens», www.droit-technologie.org; A. STROWEL, «Liaisons dangereuses et bonnes liaisons sur l'internet – À propos des hyperliens», *A. & M.*, 1998, pp. 296-308; Th. VERBIEST, «La responsabilité des outils de recherche sur internet en droit français et en droit belge», *Cahiers Lamy – droit de l'informatique et des réseaux*, 1999, n° 116, pp. 6-14.

(30) En sus de cela, l'art. 26 de la loi érige également en infractions une série d'actes contraires aux dispositions de la loi. Il est ainsi prévu, notamment, une sanction spécifique pour le *spamming* (la publicité non sollicitée envoyée par courrier électronique).

(31) Dans les travaux préparatoires, il est relevé que les questions en la matière se présentent à peu près dans les mêmes termes que pour certaines formes de criminalité dématérialisée, telles que la criminalité économique, la corruption, le blanchiment (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 11).

(32) Sous réserve des régimes particuliers de personnalité active et passive ou de compétence universelle.

(33) C'est l'application de la théorie de l'ubiquité. Voy. not. C. VAN den WYNGAERT, «De toepassing van de strafwet in de ruimte. Enkele beschouwingen», *Liber Amicorum F. Dumon*, Anvers, Kluwer, 1983, p. 515; D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à internet», *op. cit.*, p. 270; Cass., 23 janvier 1979, *Pas.*, 1979, I, p. 582; Cass., 4 février 1986, *Pas.*, 1986, I, p. 671; Cass., 16 mai 1989, *Pas.*, 1989, I, p. 973.

tel, sur le plan théorique, l'application de la règle de l'ubiquité à la criminalité informatique ne pose pas de problème (34). En pratique toutefois, il y a fort à craindre que l'effectivité de décisions rendues dans le cadre d'infractions transnationales ne soit pas assurée. Il se peut par ailleurs qu'une même infraction relève simultanément de la compétence de plusieurs juges nationaux (en raison du fait qu'elle se serait concrétisée dans plusieurs pays), auquel cas il convient de veiller à ce que l'auteur ne soit pas condamné deux fois pour le même fait (par application du principe de *non bis in idem* tel que consacré à l'art. 13 du Titre préliminaire du Code d'instruction criminelle). Cet écueil avait été mis en lumière lors de l'une des premières applications majeures du droit pénal au domaine de l'internet, à savoir l'affaire dite *Yahoo!*, relative à une vente aux enchères sur un site américain, mais accessible depuis la France, d'objets et représentations du régime nazi (35).

6. Convention Cybercriminalité. Ainsi qu'indiqué ci-avant, la Belgique a signé, le 23 novembre 2001, la Convention cybercriminalité du Conseil de l'Europe (36).

Premier traité international sur les infractions pénales commises via les réseaux informatiques, cette Convention tend à servir de modèle juridique en vue de la définition des comportements infractionnels devant être incriminés dans les droits nationaux, mais également d'un cadre de procédure et de collaboration internationale (37). Il s'agit en effet du premier instrument de droit international conventionnel contraignant spécifiquement élaboré pour lutter contre la criminalité informatique. Elle est l'expression d'un consensus minimal des États signataires relatif à la fois à la définition des crimes et délits informatiques, aux procédures à mettre en œuvre pour obtenir les preuves des infractions et aux modalités d'organisation de la coopération multilatérale. La Convention ne crée pas un nouveau droit international de l'informatique, mais fait obligation aux États ayant ratifié le texte de prendre les mesures internes nécessaires en vue de son application. Elle est entrée en vigueur le 1er juillet 2004 (38) et a d'ores et déjà été ratifiée par 17 pays (39). À l'heure actuelle, la Belgique ne l'a pas encore ratifiée (40).

En marge de la Convention, un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a été adopté par le Comité des Ministres le 7 novembre 2002 et signé par la Belgique à Strasbourg le 28 janvier 2003 (41). Ce Protocole poursuit deux objectifs : harmoniser le droit pénal matériel dans la lutte contre le racisme et la xénophobie sur l'internet et améliorer la coopération internationale dans ce domaine. Il est entré en vigueur le 1er mars 2006.

Comme indiqué *supra*, la loi belge du 28 novembre 2000 a été modifiée en vue de transposer les dispositions de la Convention en droit belge.

7. La criminalité informatique dans l'Union européenne. Après s'être particulièrement intéressée à la question de la protection de la vie privée dans le contexte d'une intensification des flux transfrontières de données personnelles et à la criminalité dite de contenu, l'Union euro-

(34) Bruxelles (réf.), 19 février 2004, *www.droit-technologie.org*. En l'espèce, des propos diffamants avaient été perpétrés par la voie d'internet et le tribunal a considéré que «des propos diffamatoires ou calomnieux perpétrés par la voie de l'internet doivent être réputés commis partout où la diffusion de ces propos a pu être reçue et lue».

(35) Après que le Tribunal de grande instance de Paris se soit déclaré compétent et ait condamné civilement et en référé l'entreprise américaine, sur le fondement du droit français, pour des faits qui avaient été commis à partir du territoire américain, il a ordonné le filtrage des informations, de sorte que le contenu illicite en France (mais légal aux U.S.A.) ne soit plus accessible au départ de la France. Alors que la société *Yahoo! Inc.* semblait, dans un premier temps, avoir accepté de se soumettre à la décision du juge français – pourtant contradictoire avec son droit national –, elle avait obtenu d'un juge de Californie une décision «préventive» (propre au droit américain et ne connaissant pas de véritable équivalent en droit européen continental) estimant que la décision française violait le premier amendement de la Constitution américaine (liberté d'expression) et ne pouvait recevoir d'exequatur aux U.S.A. Par la suite, une association de survivants des camps nazis avait cité personnellement le PDG de *Yahoo! Inc.* devant le Tribunal correctionnel de Paris, lequel s'était considéré compétent pour juger des faits en observant que ce site était accessible aux internautes sur le territoire français (T.G.I. Paris, 26 février 2002, *R.D.T.I.*, 2002/13, pp. 76 et s., note P. VALCKE et C. UYTTENDAELE).

(36) Conv. du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, Strasbourg, Ed. Conseil de l'Europe, janvier 2002, p. 13. Différents pays non membres du Conseil de l'Europe se sont associés à la Convention. Les États-Unis, le Canada, le Japon et l'Afrique du Sud l'ont ainsi également signée. Pour une analyse de la Convention, voy. not. D. GUINIER, «Cybercriminalité : contexte et engagements relatifs à la Convention du Conseil de l'Europe», *Expertises*, 2001, n° 245, pp. 56 et s.; P. VAN EECKE et J. DUMORTIER, «De implementatie van het Europese Verdrag cybercriminaliteit in de Belgische wetgeving», *Computerr.*, 2003/2, pp. 123 et s.

(37) Pour une étude des initiatives nationales et internationales relatives à la lutte contre la criminalité informatique avant l'adoption de la Convention, voy. U. SIEBER, *Information Technology Crime – National Legislations and International Initiatives*, Ius Informationis, Köln, Carl Heymanns Verlag KG, 1994.

(38) Soit après qu'elle a été ratifiée par 5 pays signataires, dont au moins trois pays membres.

(39) La liste des pays signataires ayant ratifié le texte est disponible sur le site du Conseil de l'Europe.

(40) Le texte n'a fait l'objet ni d'une loi d'assentiment, ni d'une ratification par le Roi. Il n'est donc pas encore en vigueur dans l'ordre juridique interne.

(41) La raison pour laquelle ces dispositions n'ont pas été intégrées dans la Convention elle-même figure dans le rapport explicatif du Protocole : «Le comité chargé de rédiger la Convention a examiné la possibilité d'inclure des infractions liées au contenu autres que la pornographie enfantine, comme la diffusion de propagande raciste par le biais de systèmes informatiques. Toutefois, le comité n'a pas pu parvenir à un consensus concernant l'incrimination d'un tel comportement. Alors que beaucoup de délégations se sont déclarées favorables à l'idée d'en faire une infraction pénale, plusieurs se sont dites très préoccupées par cette démarche qui porterait atteinte à la liberté d'expression (...)» (Rapport explicatif, point 4).

péenne s'est finalement penchée sur la question de la criminalité informatique. La décision-cadre du Conseil relative aux attaques visant les systèmes d'information a ainsi été adoptée en 2005 (42). Elle vise à renforcer la coopération entre États membres par un rapprochement des règles pénales réprimant les attaques contre les systèmes d'information et à garantir que des attaques contre des systèmes d'information soient passibles, dans tous les États membres, de sanctions pénales effectives, proportionnées et dissuasives. Elle entend enfin améliorer et favoriser la coopération judiciaire en supprimant les complications potentielles.

8. Plan de la contribution. La présente contribution s'attache à analyser, dans un premier temps (sect. 1), les préventions de criminalité informatique spécifique, à savoir :

§ 1. le faux informatique et l'usage de faux informatique (C. pén., art. 210*bis*);

§ 2. la fraude informatique (C. pén., art. 504*quater*);

§ 3. l'accès non autorisé à un système informatique (*hacking*) et infractions voisines (C. pén., art. 550*bis*);

§ 4. le sabotage informatique et infractions voisines (C. pén., art. 550*ter*);

§ 5. le refus d'information et de collaboration (C. instr. crim., art. 88*quater* et 90*quater*, §4).

Dans un deuxième temps (sect. 2), et brièvement, nous aborderons également quelques questions relatives à l'application de dispositions de droit pénal commun à des comportements commis par l'intermédiaire de systèmes informatiques.

Section 1. – Criminalité informatique spécifique

§ 1. – Faux informatique – Usage de faux informatique (C. pén., art. 210*bis*)

9. Genèse de la disposition. Le faux informatique et l'usage de faux informatique ont été introduits dans le Code pénal à l'article 210*bis* par la loi du 28 novembre 2000. Comme indiqué *supra*, une majorité de la jurisprudence et de la doctrine considérait, avant l'adoption de la loi, que de fausses données informatiques, tel un mot de passe détourné, ne

(42) Décision-cadre 2005/222/JAI du Conseil, du 24 février 2005, relative aux attaques visant les systèmes d'information, *J.O.U.E.*, L 69 du 16 mars 2005. Cette décision-cadre est entrée en vigueur le 16 mars 2005 et devait être transposée dans les ordres juridiques internes pour le 16 mars 2007.

constituaient pas une écriture au sens des articles 193 et suivants du Code pénal. C'est en vue de passer cet obstacle que le législateur a incriminé particulièrement le faux informatique, indépendamment du faux en écritures, même si, nous le verrons, la prévention de faux informatique emprunte à maints égards les enseignements développés à l'enseigne du faux en écritures (43).

I. – *Éléments constitutifs*

10. Le faux informatique sur le plan matériel. Le faux informatique (44) suppose une altération de la vérité par l'introduction, la modification ou la suppression de données dans un système informatique ou la modification, par tout moyen technologique, de l'utilisation possible de ces données entraînant une modification de la portée juridique des données. Ces trois conditions sont cumulatives.

11. Une altération de la vérité. Élément essentiel de l'incrimination (45) relevant de l'appréciation souveraine du juge du fond (46), la réalisation d'un faux informatique suppose avant tout une altération de la vérité (47), comme le précise l'article 210*bis*, qui sanctionne «*celui*

(43) Si la définition d'une infraction et l'analyse de ses éléments constitutifs doivent être tirés exclusivement du texte qui lui donne naissance, la détermination des dimensions matérielles et morales de l'infraction de faux informatique ne pourra faire l'économie d'un rapprochement du faux informatique de l'infraction de faux en écritures de droit commun. Trois éléments induisent ce rapprochement. Premièrement, l'art. 210*bis* a été introduit dans le chapitre IV du titre III (livre 2) du Code pénal relatif aux faux commis en écritures. Deuxièmement, ce chapitre relatif aux faux a été, à cette occasion, rebaptisé. Enfin, l'art. 193 du C. pén. lui-même a été modifié. Tout ceci souligne à suffisance l'intention du législateur d'appliquer aux faux informatiques les principes de l'art. 193 ainsi que ses développements doctrinaux et jurisprudentiels. Il en découle que la définition du faux informatique et son interprétation doivent être déterminées à la lumière de la définition du faux en écritures de droit commun. Il suffit, pour s'en convaincre, de lire dans l'exposé des motifs de la loi du 28 novembre 2000, à propos du faux informatique, que : «Dans le cadre de ce projet de loi, on ne touche pas à l'équilibre existant au niveau des dispositions relatives au faux et les autorités judiciaires disposent d'une base claire pour pouvoir aborder les formes de faux, comme la fabrication de cartes de crédit fausses ou falsifiées ou le faux en matière de contrats numériques [...]» (Projet de loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 14).

(44) Pour une étude approfondie de cette incrimination, voy. O. Leroux, «Le faux informatique», *J.T.*, 2004, pp. 509 et s.

(45) De même que l'altération de la vérité a été considérée comme relevant de l'essence même de l'infraction de faux en écritures traditionnel (voy. not. R. Garraud, *Traité théorique et pratique de droit pénal français*, 2e éd., Paris, Ed. Larose, 1898, n° 1325; J.-J. Haus, *Principes généraux du droit pénal belge*, t. II, p. 215, n° 25; J. Nypels, *Législation criminelle de la Belgique*, t. II, p. 215, n° 25; *R.P.D.B.*, v° Faux, n° 6; M. Rigaux et P.-E. Trousse, «Les crimes et les délits du Code pénal», t. III, *Les faux en écritures*, Bruxelles-Paris, Bruylant-L.G.D.J., 1957, p. 152; A. Masset, «Faux commis dans les écritures et les dépêches télégraphiques», in *Les Novelles, Droit pénal*, t. II, n° 1454-2637; Cass., 24 septembre 1951, *Pas.*, 1952, I, p. 9; Cass., 22 juillet 1970, *Pas.*, 1970, I, p. 969), le mensonge réalisé par un des modes légaux se situe au fondement de l'incrimination de faux informatique.

(46) Cass., 3 novembre 1958, *Pas.*, 1959, I, p. 233.

(47) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 14

qui commet un faux, en introduisant, dans un système informatique, en modifiant ou effaçant des données [...]», autrement dit le faussaire ayant agi par le biais de l'informatique.

Cette notion de «faux» ne bénéficie d'aucune définition légale. Concernant le faux en écritures de droit commun, c'est la jurisprudence et la doctrine qui en ont défini les contours (48). La Cour de cassation a ainsi précisé que la première condition du faux, c'est qu'il soit une imitation ou une modification de la vérité (49). Toutes les déclarations volontairement inexactes ne constituent donc pas des faux (50). Il ne peut être question de faux que si, sur un support protégé par la loi, la vérité est dissimulée d'une manière décrite par la loi (51). Ainsi, il faut notamment que l'écrit falsifié serve ou puisse servir de fondement à l'exercice d'un droit ou d'une action, à constater ou à prouver un droit (52). Le fondement ultime et la limite extrême justifiant l'incrimination du faux en écritures consiste précisément dans la nécessité de garantir la confiance que les citoyens ou l'autorité ont en la justesse et la véracité de certains actes ou faits, qui sont nécessaires pour les relations sociales (53). L'altération de la vérité ne devient un faux que lorsqu'elle est susceptible de faire naître, à l'égard des tiers, des droits dont ces derniers seraient dans l'impossibilité pratique de vérifier l'exactitude (54).

Concernant le faux informatique, la notion de «faux» semble devoir être entendue de manière large, puisque l'exposé des motifs le présente comme toute «dissimulation intentionnelle de la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique» (55), ou encore comme «toute falsification, par le biais de la manipulation de données, de données informatiques pertinentes» (56). L'ensemble des données stockées, traitées ou transmises par un système informatique tombent potentiellement sous le coup de l'article 210*bis*. Il importe peu qu'il s'agisse de données sur un disque dur ou sur un support optique ou numérique, ou simplement transmises sur un réseau (57).

Toutefois, de même que tout mensonge écrit n'est pas constitutif d'un faux en écritures, toute manipulation de données informatiques fausses ne constituera pas nécessairement un faux informatique : seules les modifications de données ayant une portée juridique altérée par la modification tomberont sous le coup de l'incrimination (58). Il appartiendra aux cours et tribunaux de définir les contours exacts de cette exigence (59).

12. L'introduction, la modification ou la suppression de données dans un système informatique ou la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique. La loi ne définit ni la notion de «données» ni celle de «système informatique» (60). Aux termes de l'exposé des motifs, il s'agit là toutefois d'une démarche volontairement elliptique : «L'avant-projet de loi ne contient aucune définition. Cela ne correspond pas à notre tradition juridique et cela produirait d'ailleurs un effet contre-productif. Aussi la terminologie employée est-elle particulièrement neutre du point de vue technologique afin d'éviter que les concepts soient trop rapidement dépassés par l'évolution de la technologie de

(48) Concernant l'altération de la vérité dans le cadre du faux en écritures de droit commun, la Cour de cassation avait précisé : «Pour l'existence du faux en écritures et de l'usage de faux, il est requis, d'une part, que l'écrit fasse preuve dans une certaine mesure de ce qu'il contient ou constate, c'est-à-dire qu'il s'impose à la confiance publique, de sorte que l'autorité ou les particuliers qui en prennent connaissance ou auxquels il est présenté, puissent être convaincus de la réalité de l'acte ou du fait juridique constaté par cet écrit ou soient en droit de lui accorder foi et, d'autre part, que l'altération de la vérité, commise avec une intention frauduleuse ou à dessein de nuire, d'une des manières prévues par la loi, soit par des mentions inexactes, soit en omettant intentionnellement de mentionner certains éléments lors de l'établissement de l'écrit, puisse causer un préjudice» (Cass., 16 juin 1999, *Pas.*, 1999, p. 362).

(49) Cass., 24 septembre 1951, *Pas.*, 1951, I, p. 9.

(50) *Pand. b*, v° Faux, n° 170; J.S.G. NYPELS et J. SERVAIS, *Le Code pénal belge interprété*, Bruxelles, Bruylant, 1896, t. I, p. 602, n° 18.

(51) Anvers, 23 septembre 1994, *T.M.R.*, 1995, p. 24, note L. LAVRYSEN.

(52) Cass. (ch. réun.), 23 décembre 1998, *Arr. cass.*, 1998, p. 1166; *A.J.T.*, 1998-1999, p. 541; *Bull.*, 1998, p. 1256; *J.L.M.B.*, 1999, p. 61; *R.W.*, 1998-1999, p. 1309; *Rev. dr. pén.*, 1999, p. 393 : «Pour tomber dans le champ d'application des articles 193 et suivants du Code pénal, il n'est pas requis que l'écrit privé ait une valeur probante légale ou procédurale; il suffit que l'écrit soit dans la vie sociale normale susceptible de faire preuve, dans une certaine mesure d'un acte ou d'un fait juridique, c'est-à-dire de convaincre ceux qui prennent connaissance de l'écrit de l'exactitude de cet acte ou de ce fait (art. 193 et 196 C. pén.)».

(53) Corr. Hasselt, 23 octobre 1985, *R.W.*, 1985-1986, col. 2356, note L. DUPONT, «Valsheid in geschriften en de openbare trouw»; Corr. Anvers, 21 septembre 1994, *T.M.R.*, 1995, p. 62.

(54) Cass., 27 septembre 1988, *Arr. cass.*, 1988-1989, p. 105; *Bull.*, 1989, p. 93; *Pas.*, 1989, I, p. 93; Cass., 5 février 1997, *Arr. cass.*, 1997, p. 166; *Bull.*, 1997, p. 173; *Pas.*, 1997, I, p. 173.

(55) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 14.

(56) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0213/004, p. 5.

(57) Concernant les données stockées sur un support optique ou numérique (CD-Rom, disquette ...), celles-ci ne tomberont sous le coup de la disposition que pour autant qu'elles soient exécutées sur un système, un CD-Rom ou une disquette seuls ne constituant pas des systèmes informatiques à proprement parler. C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 623, note 55.

(58) L'intérêt protégé par l'incrimination du faux informatique est la foi publique (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0213/001, p. 10).

(59) Le tribunal correctionnel de Dendermonde a décidé le 28 novembre 2005 que la création, avec intention frauduleuse au dessein de nuire, d'un compte de courrier électronique au nom d'une autre personne et l'envoi d'e-mails à des tiers à partir de cette adresse constituait une manipulation de données informatiques ayant une portée juridique (Corr. Dendermonde, 28 novembre 2005, *R.A.B.G.*, 2007, p. 427; *T.G.R.*, 2007, p. 57; *NjW*, 2006, p. 229, note J.D.).

(60) Comme le souligne le Conseil d'État dans son avis, cette absence de définition appelle une objection au regard du principe de la légalité des incriminations : «Dès l'instant où l'auteur du projet entend, sur le plan pénal, protéger ces 'données', il convient que ce dispositif définisse clairement ce qu'elles recouvrent exactement. Un exposé des motifs ne peut suffire» (Avis de la section législation du Conseil d'État, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0213/001, p. 53).

l'information» (61). Tout au plus retrouve-t-on dans l'exposé des motifs, et donc en dehors du texte légal lui-même, des ébauches de définitions des termes «données» et «système informatique». Concernant les données, l'exposé des motifs indique que : «Par données, on entend les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique. [...] La forme matérielle que revêtent ces données – qu'elles soient électromagnétique, optique ou autre – n'a pas d'importance pour l'avant-projet de loi» (62). Quant à ce qu'il y a lieu d'entendre par «système informatique», le même texte précise que : «Par système informatique, on entend tout système permettant le stockage, le traitement ou la transmission de données. À ce propos, on pense principalement aux ordinateurs, aux cartes à puces etc., mais également aux réseaux, et à leurs composants, ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information» (63). Outre qu'elles sont dénuées de véritable protection légale, puisqu'elles ne figurent pas dans le corps du texte de la loi elle-même, ces définitions ne sont guère satisfaisantes, car elles ne se suffisent pas à elles-mêmes : la notion de «données informatiques» est définie par rapport à celle de «système informatique» et inversement. Il n'est donc pas inutile d'éclairer ces notions au moyen des définitions qu'en a données le Conseil de l'Europe, qui décrit un système informatique comme «tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ou d'autres fonctions» et les données informatiques comme «toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un certain traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction» (64).

Quant aux notions «d'introduction», «modification» et «suppression» de données, elles ne sont pas non plus définies dans le texte de la loi et ne sont jamais explicitées dans les travaux parlementaires. Tout au plus retrouve-t-on dans les travaux préparatoires que «les manipulations des données doivent s'entendre de la manière la plus large qui soit» (65). Il semble donc qu'il faille leur prêter la signification la plus large que ces notions connaissent dans le langage courant (66).

(61) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 12.
(62) *Ibid.*
(63) *Ibid.*
(64) Conv. du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, signée à Budapest le 23 novembre 2001, Strasbourg, Ed. du Conseil de l'Europe, janvier 2002, p. 13.
(65) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 50 0213/001, p. 14.

Parmi les formes de réalisation que peut prendre le faux informatique, les travaux préparatoires citent, à titre d'exemple, la confection de fausses cartes de crédit ou la falsification de cartes de crédit, la création de faux contrat numérique ou l'introduction (dans un système informatique) d'un faux numéro de carte de crédit (67). On pourrait également citer la modification des données salariales par un employé dans la comptabilité informatique de l'entreprise, le trucage des heures supplémentaires encodées, la falsification d'une signature électronique ou l'ouverture d'un compte e-mail au nom d'une autre personne et l'envoi d'un e-mail au départ de cette adresse (68), notamment. Relèvent également du faux informatique, mais aussi, le cas échéant, de l'escroquerie, les opérations de *phishing* (69).

Outre «l'introduction», la «modification» ou la «suppression» de données dans un système informatique, la loi incrimine également la «modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique». Quelles hypothèses cette assertion vise-t-elle? Il semblerait qu'encore une fois, le législateur ait eu peur d'enserrer la nouvelle disposition dans un cadre trop strict et trop dépendant des développements technologiques, de sorte qu'il a fait le choix de compléter le texte d'une formulation alternative quant à la façon dont l'altération de la vérité doit être accomplie pour entraîner la réalisation de l'infraction. La «modification» peut ainsi être réalisée par tout moyen technologique, fût-il issu d'une technique encore inconnue. Il est à noter à ce propos que la modification qui est ici visée n'est pas une modification des données, mais bien une modification de l'utilisation qui peut être faite de données dans un système informatique. En cela, cette deuxième branche de l'alternative n'apparaît pas redondante

(66) On notera que la loi du 15 janvier 1990 relative à l'organisation d'une Banque-Carrefour de la sécurité sociale (*M.B.*, 22 février 1990), qui incrimine, en ses art. 61, 7°, et 63, 8°, l'introduction de fausses données dans la Banque-Carrefour, ne définit pas non plus la notion d'introduction de données.
(67) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 14.
(68) Corr. Dendermonde, 28 novembre 2005, *op. cit.*
(69) Pratique consistant à tromper l'utilisateur d'un système informatique en vue de lui faire communiquer des données personnelles et confidentielles (numéro de carte de crédit, numéro de carte d'identité ou de registre national, mot de passe ...), le plus souvent par l'envoi d'un courrier électronique usurpant l'identité de banques, fournisseurs de services en ligne ou sites marchands. Sur le *phishing* en droit français, voy. not. B. AMAUDRIC DU CHAUFFAUT et T. LIMOUZIN-LAMOTHE, «Une nouvelle forme de criminalité informatique à l'épreuve de la loi : le *phishing*», *Expertises*, avril 2005, pp. 140-144; N. MARTIN, «*Phishing : What's happening ?* Quelles solutions juridiques pour lutter contre le *phishing* ?», *Expertises*, février 2006, pp. 65-67.

avec la première. Au contraire, elle élargit le champ d'application de la disposition en posant qu'en l'absence d'introduction, modification ou suppression de données dans un système informatique, un faux informatique pourrait malgré tout être matériellement réalisé rien qu'en modifiant, par tout moyen technologique, l'utilisation qui peut être faite des données.

Quel que soit le mode de réalisation de l'infraction, il apparaît qu'à la différence du faux en écritures de droit commun, le faux informatique ne se réalisera pas par omission (70) : la non-introduction de données ou le manque de certaines données ne devraient pouvoir conduire à une incrimination de faux informatique.

13. Une modification de la portée juridique des données. Concernant le faux en écritures de droit commun, une jurisprudence constante, appuyée par une doctrine unanime, a toujours considéré que le préjudice (71), fût-il simplement possible (72), faisait partie des conditions d'existence de l'infraction et constituait même la «clé de voûte» de la répression du faux en écritures (73).

(70) Bien que CHAUVEAU et HÉLIE aient en leur temps exprimé des doutes quant à la possibilité de commettre un faux par omission, le texte ne le prévoyant pas explicitement (A. CHAUVEAU et F. HÉLIE, *Théorie du Code pénal*, Bruxelles, Bruylant, 1863, n^{os} 1473 et 1474), la jurisprudence l'a depuis largement admis (Cass., 29 octobre 1973, *Pas.*, 1974, I, p. 221; Corr. Gand, 5 octobre 1998, *T.M.R.*, 1999, p. 319, note : «Le faux intellectuel, visé à l'article 195, al. 3 du Code pénal, peut également résulter en dehors des constatations effectives de l'acte, des carences dont l'objectif et le résultat donnent à un fait mensonger l'apparence de la vérité»; Cass., 16 juin 1999, *Pas.*, 1999, p. 392; *Arr. cass.*, 1999, p. 392).

(71) Cass., 27 septembre 1988, *Pas.*, 1989, I, p. 93; *Arr. cass.*, 1988-1989, p. 105; *Bull.*, 1989, p. 93; Corr. Gand, 5 octobre 1998, *T.M.R.*, 1999, p. 319 : «Le préjudice à prendre pénalement en considération dans le faux en écritures consiste, d'une part, en l'offense faite à la foi publique et/ou en la violation de l'authenticité de l'écrit et, d'autre part, en la violation du droit qui devait être garanti par l'écrit».

(72) Cass. (aud. plén.), 16 juin 1999, *Pas.*, 1999, p. 362; *Arr. cass.*, 1999, p. 845; *Bull.*, 1999, p. 873; *Rev. dr. pén.*, 2000, p. 81.

(73) Bien que le texte de 1810 n'y fasse pas expressément référence, la jurisprudence a traditionnellement tiré de l'adverbe «frauduleusement» la conclusion que le préjudice constituait assurément une condition d'existence de l'infraction. Ainsi, selon la Cour de cassation, pour être punissable, le faux requiert l'existence d'un préjudice : en l'absence de préjudice effectif, il suffit d'un préjudice possible au moment où s'est produit le commencement d'exécution du faux (Cass., 30 juin 1924, *Pas.*, 1924, I, p. 437; Cass., 17 janvier 1955, *Pas.*, 1955, I, p. 508), même si aucun dommage ne se réalise ultérieurement (Cass., 11 décembre 1967, *Pas.*, 1968, I, p. 483; Cass., 3 décembre 1973, *Pas.*, 1974, I, p. 358; Cass., 16 juin 1999, *Pas.*, 1999, p. 362; J.-J. HAUS, *Principes généraux du droit pénal belge*, t. II, *op. cit.*, p. 184, n° 25, et p. 273, n° 19). Ce préjudice peut être matériel (Cass., 5 février 1951, *Pas.*, 1951, I, p. 363; Cass., 23 septembre 1963, *Pas.*, 1964, I, p. 74) ou moral (Cass. fr., 12 novembre 1813, *Bull.*, n° 247; J.S.G. NYPELS et J. SERVAIS, *Le Code pénal belge interprété*, *op. cit.*, t. I, p. 557, n° 14). La Cour de cassation a par ailleurs décidé que le fait, pour la défense, de ne pas développer d'arguments visant à contester l'existence d'un préjudice pouvait suffire pour conclure à l'existence de ce préjudice : «Lorsque le prévenu n'a pas soutenu en conclusions que l'usage de permis de conduire étrangers falsifiés ne pouvait causer un préjudice quelconque, le juge motive régulièrement et justifie légalement sa décision de condamnation en constatant que les faits imputés au demandeur [...] sont établis» (Cass., 26 novembre 1997, *Pas.*, 1997, I, n° 507; *Bull.*, 1997, II, p. 1629).

Concernant le faux informatique, il semble que cette exigence d'un préjudice s'en trouve nuancée, puisque l'article 210*bis* pose que l'infraction ne sera réalisée que pour autant que la manipulation de données ait entraîné une «modification de la portée juridique des données», catégorisant ainsi l'infraction en infraction à résultat (74). Il s'agit d'une condition nécessaire de l'incrimination, qui devra être constatée *in concreto* par le juge du fond (75). À défaut d'un tel résultat, la modification de données n'est pas constitutive d'un faux informatique mais, le cas échéant, d'une tentative de faux informatique (*cf. infra*).

Il va de soi que la portée juridique à laquelle il est fait référence doit s'entendre comme étant la portée juridique des données modifiées, prises dans leur ensemble : des données informatiques ramenées à leur unité ne peuvent bénéficier d'aucune portée juridique; c'est leur association qui peut en avoir. Une donnée informatique par elle-même n'a en effet pas de signification. Elle n'est qu'une impulsion. C'est une des raisons pour lesquelles le terme de «données» figure toujours au pluriel dans le texte de la loi.

14. Élément moral. La réalisation du faux informatique suppose le dol spécial (76), à savoir la conscience d'altérer la vérité doublée soit d'une intention frauduleuse soit du dessein de nuire, si bien que les seules erreurs, négligences ou imprudences ne sont pas punissables sur la base de l'article 210*bis* du Code pénal (77). La création de fausses cartes de crédit ou de fausses signatures à des fins scientifiques ou professionnelles ne tombe pas non plus sous le coup de la disposition (78).

15. Une intention frauduleuse. L'intention frauduleuse doit être entendue comme étant «l'intention de se procurer à soi-même ou de

(74) Voy. dans le même sens, C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 624.

(75) Ainsi que le précisent les travaux préparatoires de la loi : «Il appartiendra au juge d'apprécier si cette modification a effectivement eu lieu (...) que ces données aient réellement une portée juridique et qu'elles s'imposent dès lors à la foi publique sont des questions de fait qu'il appartient au juge du fond d'apprécier» (Exposé des motifs, *Doc. parl.*, Ch. repr., 1999-2000, sess. ord., n° 50 0213/001, p. 14).

(76) *Contra* : J.D., note sous Corr. Dendermonde, 28 novembre 2005, *NjW*, 2006, p. 231.

(77) Par analogie avec le faux en écritures : l'établissement d'un écrit objectivement contraire à la vérité avec légèreté et négligence ne peut pas constituer un faux en écritures (Corr. Charleroi, 4 octobre 1984, *R.R.D.*, 1985, p. 89).

(78) Voy., dans le même sens, F. de VILLENFAGNE et S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A. & M.*, 2001, p. 66.

procurer à autrui un profit ou un avantage illicite» (79) «sans distinction entre le cas où il est porté atteinte à un intérêt privé et celui où il est porté atteinte à un intérêt public» (80). Le profit ou l'avantage illicite est celui, de quelque nature qu'il soit, qui n'aurait pas été obtenu si la vérité et la sincérité de l'écrit avaient été respectées (81).

Pour l'établissement de l'infraction, il est sans importance que le profit ou l'avantage poursuivi ait été effectivement obtenu ou non (82). Toutefois, lorsque le faux informatique aura été commis dans le but d'obtenir un avantage patrimonial frauduleux et utilisé à cette fin, celui-ci constituera également un cas de fraude informatique (83). Ceci illustre deux des nombreux cas de concours auxquels l'application croisée des dispositions de la loi relative à la criminalité informatique ne manquera pas de conduire.

16. Le dessein de nuire. Le dessein de nuire vise la volonté de nuire à une personne physique ou morale, la nuisance pouvant être matérielle ou morale (84). Il suppose l'intention de porter atteinte aux droits de la société ou des particuliers, et spécialement, en ce qui concerne ces derniers, d'attenter à leur personne ou à leur liberté, de les attaquer dans leur honneur ou leur considération, de détruire ou de dégrader leurs biens (85). Cet élément intentionnel est distinct de la réalisation ou de la possibilité d'un préjudice (86), de même qu'il est à différencier du mobile (87). Le dessein de nuire n'exige pas que l'auteur ait agi en vue de tirer profit de son acte (88); il existe indépendamment de tout résultat (89).

(79) Cass., 8 mai 1939, *Pas.*, 1939, I, p. 229; Cass., 28 septembre 1953, *Pas.*, 1954, I, p. 48; Cass., 26 septembre 1955, *Pas.*, 1956, I, p. 47; Cass., 20 novembre 1973, *Pas.*, 1973, I, p. 310; *Arr. cass.*, 1974, I, p. 325; Cass., 22 février 1977, *Pas.*, 1977, I, p. 659; *Arr. cass.*, 1976-1977, p. 682; Cass., 2 juin 1981, *Rev. dr. pén.*, 1982, p. 906; Cass., 15 juin 1982, *Pas.*, 1982, I, p. 1194; Cass., 3 janvier 1984, *Pas.*, 1984, I, p. 461; *Arr. cass.*, 1983-1984, p. 478; Cass., 13 mars 1996, *Pas.*, 1996, I, n° 97; *Arr. cass.*, 1996, p. 224; *Bull.*, 1996, p. 239; *Pas.*, 1996, I, p. 239; *Rev. dr. pén.*, 1996, p. 755, note.

(80) Cass., 25 avril 1960, *Pas.*, 1960, I, p. 988; *Arr. Cass.*, 1959-1960, p. 766; Corr. Courtrai, 9 février 1998, *T.W.V.R.*, 1998, p. 32.

(81) M. Rigaux et P.E. Trousse, *op. cit.*, p. 231. Corr. Charleroi, 25 octobre 1984, *J.T.*, 1984, p. 652.

(82) Cass., 10 novembre 1947, *Arr. cass.*, 1947-1948, p. 357; Cass., 28 mars 1972, *Arr. cass.*, 1972, p. 720; Cass., 18 mars 1975, *Arr. cass.*, 1974-1975, p. 807; Cass., 2 octobre 2001, *Pas.*, 2001, p. 1553; Cass., 23 avril 2002, *Pas.*, 2002, p. 986.

(83) En ce cas, trois infractions viendront en concours : faux informatique, usage de faux informatique et fraude informatique.

(84) R. Screvens, *Les Novelles, Droit pénal*, t. II, Bruxelles, Larcier, 1967, n^{os} 1622 et 1623.

(85) J.-J. Haus, *Principes généraux du droit pénal belge*, t. II, *op. cit.*, n° 306.

(86) Cass., 26 mars 1985, *R.W.*, 1985-1986, col. 666, note S. Sonck.

(87) Le mobile recouvre les motifs qui ont déterminé l'agent à agir, lesquels peuvent être tout à fait louables.

(88) M. Rigaux et P.E. Trousse, *op. cit.*, p. 229.

(89) Cass., 11 juin 1923, *Pas.*, 1923, I, p. 359.

II. – *Récidive*

17. Régime particulier de récidive. La loi du 28 novembre 2000 a affecté les articles 210*bis* (faux informatique), 504*quater* (fraude informatique), 550*bis* (accès non autorisé à un système informatique) et 550*ter* (sabotage informatique) d'un régime particulier de récidive temporaire, obligatoire et spéciale.

18. Récidive temporaire. En cas de récidive, l'article 210*bis*, §4, prévoit que la peine sera doublée si la seconde infraction est commise dans un délai de cinq ans à dater du prononcé de la condamnation relative à la première infraction. Ceci est dérogatoire aux principes de la récidive délictuelle telle que régie par l'article 56, alinéa 2, du Code pénal, qui soumet la récidive à la condition que le condamné ait «commis le nouveau délit avant l'expiration de cinq ans depuis qu'il a subi ou prescrit sa peine». Le délai d'épreuve de la récidive en matière de faux informatique s'en trouve donc réduit d'autant, puisque le point de départ de ce délai ne sera pas la fin du délai d'épreuve du sursis ou la fin de la peine, voire sa prescription, mais bien le prononcé de la condamnation elle-même.

Il n'est jamais expliqué dans les travaux préparatoires la raison pour laquelle il a été dérogé au régime général de la récidive légale. Sans doute cette particularité a-t-elle échappé au législateur lors de la rédaction du texte. Elle n'est toutefois pas sans conséquences, puisqu'alors que la récidive délictuelle pouvait être établie lorsqu'un second délit était commis dans un délai allant jusqu'à dix ans à dater du prononcé de la première peine (soit endéans le délai de cinq ans fixé par la loi pouvant prendre cours au terme d'une première période de cinq ans équivalente à la peine elle-même ou à la durée du sursis affectant cette peine), en matière de faux informatique (et il en ira de même pour les autres préventions analysées dans cette contribution – *cf. infra*), ce délai ne pourra jamais excéder cinq ans.

En outre, cela n'ira pas sans susciter quelques difficultés pratiques, dans la mesure où les avocats et les magistrats devront s'adapter à cette règle précise et ne pas évaluer la possibilité d'une récidive pour un délit informatique comme ils le font pour un délit de droit commun (notamment en ce qui concerne l'importance de la première peine, puisque, comme indiqué *infra*, celle-ci ne devra pas être d'un an au moins). Sans doute des erreurs sont-elles à craindre.

Enfin, bien que la loi ne le précise pas, la récidive spéciale ne pourra se fonder que sur une première condamnation coulée en force de chose jugée (90).

19. Récidive obligatoire. La récidive est obligatoire. Les termes de la loi prévoient en effet que les peines seront doublées en cas de récidive, sans laisser au juge la possibilité d'apprécier l'opportunité de relever les seuils de peines. Ceci est également dérogatoire au régime général de la récidive délictuelle fondée sur l'article 56, alinéa 2, du Code pénal, puisqu'aux termes de cette disposition, le juge peut prononcer une peine double du maximum prévu par la loi pour le délit mais n'y est pas tenu.

20. Récidive spéciale. La récidive est encore spéciale (ou spécifique), puisque l'article 210*bis*, §4, limite la récidive légale à la commission d'un faux informatique à la suite d'une première condamnation devenue définitive pour une *infraction informatique* (soit un faux informatique, une prise de connaissance de télécommunications privées ou une violation du secret de ces télécommunications, une fraude informatique, un accès non autorisé à un système informatique ou un sabotage informatique) (91). Une première condamnation prononcée dans le délai visé ci-avant mais pour une infraction qui n'est pas reprise au §4 de la disposition ne peut fonder une récidive spécifique.

On notera également que l'établissement de la récidive spécifique ne suppose pas, contrairement à la récidive délictuelle de droit commun telle que régie par l'article 56, alinéa 2, du Code pénal, que la première condamnation ait été d'un an au moins. La loi ne prévoit en effet pas cette condition. Il s'en déduit qu'un récidiviste en matière de criminalité informatique pourrait encore voir sa seconde peine assortie d'un sursis dans l'hypothèse où la première condamnation n'aurait pas excédé douze mois. En matière de récidive fondée sur l'article 56, alinéa 2, du Code pénal, cela ne serait pas possible, étant donné que cette récidive se fonde sur une première condamnation à un an au moins, soit un seuil

(90) On notera à ce propos que l'art. 56, al. 2, du C. pén. ne prévoit pas non plus explicitement cette condition. La Cour de cassation avait toutefois décidé que cette condition était nécessaire pour que le défendeur ne puisse se plaindre, ni d'une appréciation arbitraire de son passé, ni de n'avoir pas été solennellement averti du risque qu'il encourait en accomplissant une nouvelle infraction (Cass., 17 juin 1980, *Pas.*, 1980, I, p. 1281; P.-L. BODSON, *Manuel de droit pénal*, Liège, Faculté de droit, d'économie et de science sociale, 1986, p. 468).

(91) On notera à ce propos qu'alors que les art. 210*bis*, 504*quater*, 550*bis* et 550*ter* du C. pén. prévoient que la récidive ne sera fondée que pour autant que ces infractions aient été commises après une première condamnation pour l'une de ces préventions ou pour violation des art. 259*bis* ou 314*bis* du même Code, le régime de récidive de ces deux dernières infractions (relatives à l'écoute, à la prise de connaissance, à l'enregistrement et au secret des communications privées) n'est pas soumis à cette même règle, de sorte que la récidive spécifique ne joue qu'à sens unique.

excédant les douze mois fixés par la loi relative à la suspension, au sursis et à la probation (92).

Enfin, on relèvera que la Cour de cassation a admis, depuis le milieu des années 1970, qu'il était possible qu'il y ait un concours entre une récidive prévue par une loi particulière et la récidive légale prévue aux articles 54 et suivants du Code pénal (93). Ainsi, la Cour avait considéré que : «Lorsque, après une condamnation du chef d'une infraction prévue par le Code pénal, le condamné commet une infraction à une loi particulière contenant des dispositions qui n'organisent la récidive que pour les infractions qui y sont prévues, est légale l'application à cette dernière infraction des dispositions du Chapitre V du Livre premier du Code pénal lorsque les conditions prévues pour la récidive spéciale ne sont pas remplies» (94). Il s'en déduit que lorsque la récidive spéciale ne trouvera pas à s'appliquer (soit parce que le délai d'épreuve aurait été dépassé et que l'infraction informatique aurait été commise après l'échéance de celui-ci ou parce que la première condamnation porterait sur une infraction ne relevant pas de la criminalité informatique, notamment), la récidive générale fondée sur l'article 56, alinéa 2, du Code pénal pourra être retenue lorsque les conditions légales de celles-ci seront remplies. La récidive des articles 54 et suivants du Code pénal est en effet une circonstance aggravante personnelle d'ordre public.

III. – *Les peines*

21. Peines délictuelles. La peine prévue par la loi pour le délit est de six mois à cinq ans d'emprisonnement et une amende comprise entre 26 et 100.000 EUR, ces peines devant être doublées en cas de récidive. Le faux informatique est donc un délit. Cela distingue nettement le faux informatique des faux en écritures de droit commun, qui, sauf les hypothèses de faux commis dans les passeports, ports d'armes, livrets, feuilles de route et certificats (95), sont passibles de peines criminelles. On relèvera également que si la peine privative de liberté a été revue à la baisse, la loi a prévu la possibilité d'infliger une amende pouvant s'élever à un montant important. Or, comme l'avait souligné le Comité européen mis en place par le Conseil de l'Europe pour étudier les impli-

(92) Art. 8, §1er, de la loi du 29 juin 1964 concernant la suspension, le sursis et la probation (*M.B.*, 17 juillet 1964; *err.* : *M.B.*, 24 juillet 1964).

(93) Cass., 4 juin 1974, *Pas.*, 1974, I, p. 1021; Cass., 2 juin 1975, *Pas.*, 1975, I, p. 941; Cass., 23 juin 1975, *Pas.*, 1975, I, p. 1025.

(94) Cons. Cass., 23 janvier 1967, *Pas.*, 1967, I, p. 611, avec concl. av. gén. CHARLES.

(95) Sous réserve de l'hypothèse visée à l'art. 208 du C. pén.

cations de la dimension informatique sur la criminalité, «la dimension informatique d'un délit ne doit pas être considérée en tant que telle comme une circonstance aggravante de celui-ci» (96).

La possibilité de sanctionner l'infraction d'une peine de travail autonome n'est bien sûr pas exclue (97).

De même, les seuils de la peine privative de liberté rendent possible la délivrance d'un mandat d'arrêt (98).

La loi n'a pas prévu de peines accessoires. Outre l'emprisonnement et l'amende, la confiscation spéciale prévue aux articles 42 et suivants du Code pénal sera toutefois applicable. Il sera donc possible pour le juge, le cas échéant, de prononcer, accessoirement à la peine principale, la confiscation du matériel informatique utilisé pour commettre l'infraction ainsi que de tous ses périphériques et accessoires présentant un lien de convenance avec la commission de l'infraction. Il en irait ainsi, notamment, des supports de mémoire contenant les données faussées, des programmes et logiciels utilisés, de cartes à puces vierges ou modifiées ...

On notera encore que la loi n'a pas prévu la possibilité pour le juge de prononcer une interdiction sur la base des articles 31 et suivants du Code pénal. De même, le faux informatique n'a pas été ajouté à la liste des infractions reprises à l'article 1er de l'arrêté royal relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines professions ou activités (99). Il n'est donc pas possible pour le juge correctionnel d'assortir sa condamnation pour des faits de faux informatique d'une interdiction d'exercer personnellement ou à l'intermédiaire de tiers les fonctions d'administrateur, de commissaire ou de gérant d'une société privée, alors même que cette possibilité lui est ouverte lors de condamnation pour des faits de faux en écritures et d'usage de faux en écritures, que ce soit en qualité d'auteur ou de complice, et alors même qu'il se serait agi d'une simple tentative. Sans doute serait-il opportun, pour une plus grande cohérence de la disposition, que l'article 210*bis* du Code pénal soit ajouté à cette liste.

(96) Rapport accompagnant la Recommandation n° R(89)9 sur la criminalité en rapport avec l'ordinateur, Strasbourg, 1990, p. 23.

(97) Conformément à l'art. 37*ter*, §1er, al. 2, du C. pén.

(98) Art. 16, §1er, al. 1er, de la loi du 20 juillet 1990 relative à la détention préventive.

(99) A.R. n° 22 du 24 octobre 1934 relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines professions ou activités (*M.B.*, 27 octobre 1934).

IV. – *Questions particulières de droit pénal*

A. *Tentative*

22. Incrimination de la tentative de faux informatique. La tentative de faux informatique est visée à l'article 210*bis*, §3, qui prévoit une peine comprise entre six mois et trois ans de prison et/ou une amende allant de 26 à 50.000 EUR (100).

Dans la pratique, il pourra s'avérer difficile de faire le départ entre des actes simplement préparatoires (qui ne relèvent pas de la tentative punissable) et des actes d'exécution. En effet, sauf les cas où les actes préparatoires ne consisteront pas en une introduction, une modification ou une suppression de données dans un système informatique (ou dans la modification de l'utilisation possible des données), les uns comme les autres de ces actes s'exécuteront selon un *modus operandi* tout à fait similaire (à savoir une introduction, une modification ou une suppression de données ou une modification de l'utilisation possible des données), dans un *continuum* difficilement sécable, et ce, contrairement à bon nombre d'infractions de droit commun qui supposent que l'agent ait préalablement posé certains actes de nature fort différentes avant d'être en mesure de commettre le délit ou le crime.

23. Pas d'incrimination de la tentative d'usage de faux informatique. Curieusement, la tentative d'usage de faux informatique n'est pas incriminée. Sans doute s'agit-il d'un oubli du législateur (101).

24. Faux informatique unique. On relèvera encore que, bien que le gouvernement ait exprimé le souhait de réprimer de la même manière un délit commis en ligne ou hors ligne (102), la loi relative au faux informatique ne reprend pas la distinction établie pour le faux en écritures de droit commun entre la nature des actes falsifiés (acte public, acte authentique, commercial ou privé (103)), ni quant à la qualité de

(100) Et ce, conformément à l'art. 53 du C. pén., qui prévoit qu'en matière délictuelle, c'est la loi qui détermine les cas dans lesquels la tentative de délit est punissable.

(101) On relèvera que l'art. 11 de la Convention cybercriminalité impose aux États signataires d'incriminer la tentative de falsification informatique visée à l'art. 7 de ladite Convention. Par ailleurs, le texte de l'art. 210*bis* contient manifestement un mot de trop, puisque le §3 est rédigé comme suit : «La tentative de commettre l'infraction visée au §1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement». Ce «et», qui n'a pas de sens dans la phrase, ne se retrouve pas dans la version néerlandaise du texte.

(102) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 10.

(103) Les écritures privées peuvent être considérées comme les écritures résiduaires. Elles ne sont ni authentiques, ni publiques, ni commerciales, ni bancaires. A. De Nauw, *Initiation au droit pénal spécial*, 2e éd., Bruxelles, Story-Scientia, 1987, p. 33.

l'auteur de l'infraction (fonctionnaires dans l'exercice de leurs fonctions ou non). Interpellé par le Conseil d'État (104) qui critiquait ce choix, le gouvernement avait justifié cette omission par la volonté de dépasser la complexité des dispositions de droit commun en matière de faux (concernant la distinction selon la nature de l'acte falsifié et selon l'auteur) (105). Cette différence de traitement selon que le faux est réalisé par l'intermédiaire d'un système informatique ou non incitera sans doute un jour les plaideurs à solliciter de la Cour constitutionnelle qu'elle se penche sur cette question.

Dans le même ordre d'idées, il y a lieu de noter qu'alors que la tentative de faux informatique est toujours punissable, il n'en va pas de même de la tentative de faux en écritures de droit commun, qui n'est passible de sanction pénale qu'en cas de tentative de faux criminel.

B. *Usage de faux informatique*

25. Incrimination de l'usage de faux informatique. L'usage de faux informatique est incriminé par le §2 de l'article 210*bis* du Code pénal, qui prévoit que «Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux».

Pas plus que le faux informatique ou l'usage de faux en écritures de droit commun, l'usage de faux informatique ne fait l'objet d'une définition légale.

Tout comme l'usage d'écritures fausses constitue un fait distinct du faux, l'usage de faux informatique constitue une infraction indépendante de celle de faux informatique, lesquelles peuvent être poursuivies séparément devant le juge compétent (106). Il s'en déduit que la réalisation d'un faux informatique est punissable indépendamment de tout usage et inversement, et que l'auteur d'un faux informatique et l'auteur d'un usage de faux informatique peuvent avoir des coauteurs et complices distincts (107).

(104) Avis du Conseil d'état, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 51.

(105) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 14.

(106) Par analogie avec le faux en écritures de droit commun, voy. : Cass., 10 décembre 1888, *Pas.*, 1889, I, p. 60; Cass., 29 janvier 1923, *Pas.*, 1923, I, p. 175; Cass., 20 juin 1961, *Pas.*, 1961, I, p. 1155; Bruxelles, 25 novembre 1964, *Jur. Liège*, 1964-1965, p. 105; Cass., 25 juin 1980, *Pas.*, 1980, I, p. 1329; *Arr. cass.*, 1979-1980, p. 1352; *Bull.*, 1980, p. 1329; Corr. Verviers, 12 septembre 1991, *Orientations*, 1991, p. 224, note A. Masset; R. Screvens, *Les Novelles, Droit pénal*, t. II, *op. cit.*, n^{os} 2098-2100.

(107) Par analogie avec ce qui a été développé en matière de faux de droit commun : J.S.G. Nypels et S. Servais, *Le Code pénal belge interprété*, *op. cit.*, t. I, p. 616, n° 11.

Toutefois, en ce qui concerne le faux de droit commun, lorsque le faux et l'usage de faux auront été commis par le même auteur, la tendance jurisprudentielle et doctrinale majoritaire tend à ne voir dans ces faits qu'une seule infraction, celle de faux, l'usage étant alors considéré comme la continuation du faux (108). Une seconde tendance considère que le faux et l'usage de faux commis par la même personne constituent deux délits distincts, qui seront le plus souvent ramenés à l'unité, par le recours à la fiction du délit collectif, lorsqu'ils constitueront l'exécution d'une même volonté ou résolution criminelle (109). Comme le souligne A. De Nauw, le choix entre les deux opinions est, dans certains domaines, spéculatif, parce que les notions de délit continu et de délit collectif ont des conséquences parallèles (110).

Sur le plan matériel, l'usage de faux informatique suppose la réunion de deux conditions. La première condition d'existence de l'usage de faux informatique, c'est celle d'un faux informatique préexistant, réunissant les éléments constitutifs de l'infraction, dont on peut user (111). La seconde condition consiste dans l'utilisation ou l'emploi du faux informatique. Selon la Cour de cassation, concernant l'usage de faux de droit commun : «l'usage de faux est l'application de l'acte falsifié à l'emploi auquel il est destiné» (112). Pour qu'il y ait usage de faux informatique sur le plan matériel, il faut donc, mais il suffit, que les données utilisées aient constitué un faux informatique et qu'elles aient

(108) J.S.G. Nypels et J. Servais, *Le Code pénal belge interprété*, *op. cit.*, t. I, pp. 695 et s.; J.-J. Haus, *Principes généraux du droit pénal belge*, t. II, *op. cit.*, n° 560; R. Screvens, *Les Novelles, Droit pénal*, t. II, *op. cit.*, n° 2121; J.-P. Jaspar et A. Marchal, *Droit ciminel : Traité théorique et pratique*, Bruxelles, Larcier, 1975, n^{os} 575 à 579; *R.P.D.B.*, n^{os} 377 à 379 et 400 à 402; Cass., 1er février 1869, *Pas.*, 1869, I, p. 103, sur concl. conf. Faider; Cass., 18 février 1974, *Pas.*, 1974, I, p. 641; Cass., 6 février 1979, *Pas.*, 1979, I, p. 641; Bruxelles, 22 novembre 1978, *Rev. prat. soc.*, 1979, p. 67; Cass., 13 avril 1953, *Pas.*, 1953, I, p. 611.

(109) M. Rigaux et P.E. Trousse, *op. cit.*, p. 253; G. Hoornaert, *Faux en écritures et faux bilans*, Bruxelles, Bruylant, 1945, n° 15; A. De Nauw, «Valsheid in geschriften en gebruik ervan door dezelfde persoon is geen voortdurend maar wel een collectief misdrijf», *R.W.*, 1972-1973, col. 887-895; A. De Nauw, *Initiation au droit pénal spécial*, 2^{e} éd., *op. cit.*, p. 52; Cass., 13 avril 1953, *Pas.*, 1953, I, p. 611; Cass., 12 mars 1956, *Pas.*, 1956, I, p. 732; Cass., 5 septembre 1957, *Pas.*, 1957, I, p. 1382; Corr. Liège, 17 juin 1964, *Pas.*, 1964, III, p. 121.

(110) A. De Nauw, *Initiation au droit pénal spécial*, 2^{e} éd., *op. cit.*, p. 52.

(111) À ce propos, la Cour de cassation avait précisé, concernant le faux en écritures de droit commun, que «ne saurait constituer l'usage d'un faux le fait que la personne poursuivie, notamment du chef de la falsification dudit acte, conteste devant le juge cette dernière prévention en soutenant que cet acte est conforme à la réalité qu'il avait pour objet de constater» (Cass., 16 juin 1987, *Pas.*, 1987, I, p. 1280; *Arr. cass.*, 1986-1987, p. 1425; *Bull.*, 1987, p. 1280). Le fait, pour la personne poursuivie, d'invoquer l'acte prétendument faux pour établir qu'il correspond à la réalité ne constitue donc pas un usage de faux (Mons, 17 octobre 1990, *Pas.*, 1991, II, p. 44). Par contre, constitue un usage de faux en écritures de droit commun, l'exercice par une personne, poursuivie pour faux en écritures, d'une action civile fondée sur l'acte argué de faux; il ne s'agit plus alors d'un moyen de défense opposé à l'action publique (Cass., 9 décembre 1992, *Pas.*, 1992, I, p. 1355; *Arr. cass.*, 1991-1992, p. 1408; *Bull.*, 1992, p. 1355).

(112) Cass., 10 janvier 1955, *Pas.*, 1955, I, p. 463.

été utilisées aux fins auxquelles elles étaient destinées (113). La loi n'ayant pas défini l'usage de faux informatique, il appartient au juge du fond d'apprécier souverainement les faits qui constituent cet usage (114).

Concernant l'élément moral de l'infraction, l'auteur de l'usage de faux informatique doit, pour être punissable, avoir fait usage du faux non seulement en connaissance de cause, mais même avec une intention frauduleuse ou un dessein de nuire. En effet, bien que l'article 210*bis* ne le mentionne pas explicitement, l'usage de faux informatique suppose un dol spécial (à savoir l'intention frauduleuse ou le dessein de nuire). Ceci peut être déduit de la concordance du libellé de l'article 210*bis* du Code pénal avec celui de l'article 197 du même Code (relatif à l'usage de faux de droit commun), qui justifie la transposition *mutatis mutandis* des éléments constitutifs de l'usage de faux de droit commun à l'usage de faux informatique (115). La simple connaissance de la falsification dont il a été fait usage ne suffit donc pas à constituer le dol spécial requis par la loi (116). De même, l'usage inconscient ou involontaire n'est pas incriminé. Pour tomber sous le coup de l'incrimination, il faut que l'auteur ait su qu'il usait d'un faux et qu'il ait été animé d'une intentionnalité caractérisée. Il appartient au ministère public de prouver cette état d'esprit. Faut-il que l'usage ait fait naître un préjudice pour qu'il soit répréhensible? Selon C. Meunier, le rapprochement devant être opéré entre le faux de droit commun et le faux informatique soumet la réalisation de cette dernière infraction à la naissance d'un préjudice possible (117).

L'auteur d'un usage de faux informatique est passible d'une peine d'emprisonnement comprise entre six mois et cinq ans et/ou d'une amende comprise entre vingt-six et cent mille euros (118). La sanction est donc la même que pour l'auteur du faux informatique lui-même.

(113) Par analogie avec le faux en écritures de droit commun : Cass., 1er juin 1920, *Pas.*, 1920, I, p. 181.

(114) Par analogie avec le faux en écritures de droit commun : Cass., 5 décembre 1949, *Pas.*, 1949, I, p. 214; Liège, 17 novembre 1981, *Jur. Liège*, 1982, p. 85.

(115) C. Meunier, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 626.

(116) Par analogie avec le faux en écritures de droit commun : Cass., 14 mars 1910, *Pas.*, 1910, I, p. 146.

(117) C. Meunier, *op. cit.*

(118) Devant être augmentée des décimes additionnels.

V. – *Questions particulières de procédure pénale*

26. Écoutes de télécommunications privées. Le faux informatique est repris dans la liste de l'article 90*ter* du Code d'instruction criminelle relatif aux infractions pour lesquelles des mesures d'écoute, de prise de connaissance ou d'enregistrement de communications et de télécommunications privées sont possibles (119). Des écoutes électroniques peuvent donc être diligentées. On entend par écoute électronique l'interception, pendant la transmission, à l'aide d'un appareillage quelconque, de télécommunications numériques privées. De telles écoutes sont techniquement et légalement possibles (120). Si le juge d'instruction ordonne la mesure, les enquêteurs auront donc la possibilité d'enregistrer et de prendre connaissance de ces messages pendant leur transmission.

27. Prescription du faux informatique et de l'usage de faux informatique. Concernant la prescription de faux en écritures de droit commun, la Cour de cassation a, par une jurisprudence constante, distingué selon que l'usage avait été le fait du faussaire ou d'un tiers (121). Lorsque le faussaire lui-même a aussi fait usage de la pièce fausse avec la même intention frauduleuse ou le même dessein de nuire, la prescription de l'action publique ne commence à courir qu'à dater du dernier fait d'usage du faux, et ce, tant à l'égard du fait de faux qu'à l'égard du fait d'usage de la pièce fausse (122). En effet, bien que le

(119) C. instr. crim., art. 90*ter*, §2, 1°*quater*.

(120) L. 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées (*M.B.*, 24 janvier 1995), mod. par L. 10 juin 1998 (*M.B.*, 22 septembre 1998), qui a remplacé les termes «communications téléphoniques» par «télécommunications» au sens de l'art. 68, 4°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

(121) Sur la question de la prescription du faux et de l'usage de faux en écritures, voy. not. J. Spreutels, F. Roggen, E. Roger France, *Droit pénal des affaires*, Bruxelles, Bruylant, 2005, pp. 251 et s.

(122) Cass., 14 décembre 1931, *Pas.*, 1932, I, p. 6; Cass., 5 septembre 1957, *Pas.*, 1957, I, p. 1382; Cass., 29 octobre 1980, *Arr. cass.*, 1980-1981, p. 226; *Bull.*, 1981, p. 253; *Pas.*, 1981, I, p. 253, note J.V.; Cass., 9 février 1982, *Pas.*, 1982, I, p. 724; *Arr. cass.*, 1985-1986, p. 917; *Bull.*, 1986, p. 834; Cass., 1er février 1984, *Pas.*, 1984, I, p. 617; *Arr. cass.*, 1983-1984, p. 668; *Bull.*, 1984, p. 617; Cass., 4 mars 1986, *Pas.*, 1986, I, p. 834; Cass., 10 janvier 1989, *Pas.*, 1989, I, p. 499; Corr. Namur, 18 décembre 1991, *R.R.D.*, 1992, p. 279; Bruxelles, 20 janvier 1992, *J.T.*, 1992, p. 329; Cass., 2 novembre 1993, *Pas.*, 1993, I, p. 912; Cass., 26 octobre 1994, *Pas.*, 1994, I, p. 860; *Arr. cass.*, 1994, p. 878 (somm.); *Bull.*, 1994, p. 860 (somm.); Liège, 24 mars 1995, *J.L.M.B.*, 1995, p. 834, obs. F. Kéfer; Cass. (ch. réun.), 23 décembre 1998, *Pas.*, 1998, p. 534; *A.J.T.*, 1998-1999, p. 541; *Arr. cass.*, 1998, p. 1166; *Bull.*, 1998, p. 1256; *J.L.M.B.*, 1999, p. 61; *R.W.*, 1998-1999, p. 1309; *Rev. dr. pén.*, 1999, p. 393; Cass., 6 octobre 1999, *Pas.*, 1999, p. 511; *Arr. cass.*, 1999, p. 1225; *Bull.*, 1999, p. 1277; *Dr. circ.*, 2000, p. 50; Cass., 12 février 2002, *NjW*, 2002, p. 169, note S. Vandromme; Cass., 24 septembre 2002, *Pas.*, 2002, p. 1728. Dans son arrêt de 1982 précité, la Cour n'a pas manqué de préciser que : «Si le faux en écritures et l'usage de la pièce fausse par le faussaire ne constituent qu'une seule et même infraction, prévue et réprimée par les articles 193 et 196 C. pén., lorsque cet usage a été accompli par le faussaire avec la même intention frauduleuse ou le même dessein de nuire que la falsification, il ne ressort d'aucune disposition légale que, dans le cas où un laps de temps plus long que

faux soit un délit instantané se consommant par l'altération ou la fabrication de l'acte (123), la jurisprudence majoritaire considère que l'usage du faux par le faussaire lui-même peut être considéré comme la continuation du faux (*cf. supra*) (124). Le faussaire risque ainsi d'être exposé longtemps aux poursuites judiciaires (125).

La loi relative à la criminalité informatique ne contient aucun dispositif particulier quant à la prescription du faux informatique. En l'absence de dispositions particulières, il apparaît que les questions relatives à la prescription du faux informatique et de l'usage de faux informatique seront appelées à bénéficier des éclairages apportés par la jurisprudence et la doctrine pour le faux en écritures de droit commun. À défaut d'usage des données fausses, le délai de prescription de l'action publique pour le faux informatique commencera à courir à dater de la réalisation du faux, c'est-à-dire à dater de l'introduction, de la modification ou de la suppression de données dans un système informatique (ou de la modification de l'utilisation possible des données). Il ne fait en effet pas de doute que le faux informatique est un délit instantané (126), lequel est complètement réalisé par l'accomplissement de l'acte défendu ou prescrit. Ce caractère instantané n'est pas affecté par le fait qu'un élément constitutif de l'infraction s'étendrait sur une certaine durée ou par la circonstance que, le fait ayant été consommé, ses effets perdurent (127).

En cas d'usage de faux informatique, il convient de distinguer selon que les données ont été utilisées par le faussaire lui-même ou par un tiers. Si l'usage est le fait du faussaire ou d'un tiers qui en userait con-

le délai de prescription s'est écoulé entre la perpétration du faux et le premier acte d'usage de celui-ci, l'auteur du faux, qui ne peut être condamné de ce chef, la prescription étant acquise, ne puisse être légalement condamné du chef du seul usage de ce faux».

(123) Cass., 25 novembre 1992, *Pas.*, 1992, I, p. 1302 : «Est instantanée l'infraction qui, telle qu'elle est définie par la loi, s'accomplit à un moment déterminé par un fait unique». H. DONNEDIEU de VABRES, *Traité élémentaire de droit criminel*, 2e éd., Paris, Sirey, 1943, n° 183; R. MERLE et A. VITU, *Traité de droit criminel*, t. I, 7e éd., Paris, Cujas, 1997, n° 490 : «Le délit instantané est celui qui s'accomplit en un trait de temps, par une action de courte durée».

(124) Cass., 23 décembre 1998, *Arr. cass.*, 1998, I, p. 1166; Cass., 6 octobre 1999, *Arr. cass.*, 1999, I, p. 1225; Cass., 12 février 2002, *Pas.*, 2002, p. 388; Cass., 24 septembre 2002, *Pas.*, 2002, p. 1728 : «L'usage d'un faux se continue, même sans fait nouveau de l'auteur du faux et sans intervention itérative de sa part, tant que le but qu'il visait n'est pas atteint et tant que l'acte initial qui lui est reproché continue de produire, sans qu'il s'y oppose, l'effet utile qu'il en attendait».

(125) Ch. HENNAU et J. VERHAEGHEN, *Droit pénal général*, Bruxelles, Bruylant, 3ème éd., 2003, p. 249.

(126) Par analogie avec le faux de droit commun, la Cour de cassation a rappelé que la possibilité d'utiliser un faux de droit commun n'a pas pour résultat la prolongation de la rédaction de ce faux (Cass., 29 février 1984, *Pas.*, 1984, I, p. 751, concl. M.P.; *Arr. cass.*, 1983-1984, p. 819; *Bull.*, 1984, p. 751, concl. M.P.; *R.W.*, 1984-1985, col. 1922, note A. VANDEPLAS).

(127) Ch. HENNAU et J. VERHAEGEN, *op. cit.*, p. 77, concernant le faux en écritures de droit commun.

formément à la volonté ou aux prévisions du faussaire, la prescription prendra cours à dater du dernier fait d'usage. Si, par contre, l'usage est le fait d'un tiers et n'a pas été voulu ou prévu par le faussaire, dans ce cas-là, chaque usage du faux informatique devra être envisagé de façon isolée pour déterminer la prise de cours du délai. À l'instar du faux, l'usage de faux informatique est en effet un délit instantané. L'analyse des éléments constitutifs de l'infraction démontre en effet à suffisance que le délit est réalisé dès qu'il a été fait usage des données fausses. Qu'en est-il maintenant de la prescription du faux ou de l'usage de faux lorsqu'il est commis en ligne? Il nous apparaît que le faux informatique demeure insensible à une éventuelle persistance des données fausses en ligne car «une infraction n'est continue que si le fait, tel qu'il a été défini par la loi, continue à se perpétrer; s'il vient à cesser dès qu'il a été commis, l'infraction, quelle que puisse être la durée du mal qu'elle entraîne, est instantanée».

§ 2. – FRAUDE INFORMATIQUE (C. PÉN., ART. 504*QUATER*)

28. Genèse de la disposition. La fraude informatique a été introduite dans le Code pénal à l'article 504*quater* par l'article 5 de la loi du 28 novembre 2000 relative à la criminalité informatique, qui punit la manipulation de données en vue de se procurer pour soi-même ou pour autrui un avantage économique illégal.

Il était devenu nécessaire d'adapter le Code pénal aux escroqueries commises par le biais de systèmes informatiques en raison du fait que l'escroquerie de droit commun était la fraude consistant à tromper la confiance de tiers. L'article 496 du Code pénal prévoyait en effet que l'escroc devait s'être fait «remettre ou délivrer» un bien, ce qui impliquait un caractère volontaire qui ne pouvait être que le fait d'un être humain (128). Or, le retrait automatique d'une somme d'argent par un utilisateur qui savait que son compte n'était pas approvisionné ne relevait pas de cette catégorie (129). De même, l'utilisation d'une carte ban-

(128) Corr. Liège, 22 mars 1982, *Jur. Liège*, 1982, p. 319. Pour une étude doctrinale et jurisprudentielle de l'applicabilité de l'art. 496 du C. pén. aux escroqueries commises à l'aide d'un ordinateur, voy. not. B. de SCHUTTER, *Informaticacriminaliteit*, Antwerpen, Kluwer rechtswetenschappen, 1988, p. 11; J. DUMORTIER, *Informatica en telecommunicatierecht*, t. I, Leuven, Acco, 1995-1996, p. 75; B. SPRUYT, «Computers op de strafbank. Analyse van het fenomeen informaticacriminaliteit : nationale en internationale strafrechtelijke perspectieven», *op. cit.*, p. 330.

(129) C'est en ce sens qu'avait tranché le Tribunal correctionnel de Liège, notamment (Corr. Liège, 22 mars 1982, *Jur. Liège*, 1982, p. 319). Pour une approche doctrinale de la fraude informatique avant l'adoption de la loi, voy. not. H.-D. BOSLY, «La fraude informatique: une approche de droit comparé», *Rev. dr. pén.*, 1985, pp. 287-306; M. BRIAT, «La fraude informatique : une approche de droit comparé»,

caire volée n'impliquait la tromperie d'une personne. Ces opérations tombent aujourd'hui certainement sous le coup de l'article 504*quater* du Code pénal, de même que, de façon plus générale, les retraits d'argent ou les achats de produits au moyen de cartes bancaires volées, falsifiées ou détournées (130).

29. Notion. La fraude informatique consiste donc en une adaptation de l'escroquerie lorsqu'un avantage économique illicite a été poursuivi par la *tromperie d'une machine* (131). Ainsi que le précise C. Meunier, «s'il apparaît que les manœuvres ont induit une personne en erreur, et non une machine, il y a lieu de privilégier l'article 496 du Code pénal réprimant l'escroquerie, éventuellement combiné avec l'article 210*bis* du Code pénal» (132). On relèvera à ce sujet qu'en cas de fraude commise à l'occasion de vente en ligne (133), les articles 498 et suivants du Code pénal trouveront à s'appliquer sans difficulté particulière.

L'article 504*quater* du Code pénal sanctionne «celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique». Constituent donc des cas de fraude informatique, l'utilisation d'une carte de crédit volée, le dépassement illicite de crédit au

Rev. dr. pén., 1985, pp. 287-306; G. Demanet, «De l'utilisation frauduleuse des cartes bancaires : une nouvelle incrimination est-elle nécessaire?», *Rev. dr. pén.*, 1985, p. 915; M. Jaeger, «La fraude informatique», *Rev. dr. pén.*, 1985, pp. 323-354.

(130) Avant l'adoption de la loi, la jurisprudence qualifiait le plus souvent ce type de fait de vol avec fausses clés (l'usage d'un code secret détourné ou du mot de passe d'un tiers relevant de cette circonstance aggravante), soit un crime passible de la réclusion de cinq à dix ans. Depuis l'entrée en vigueur de la loi, la Cour de cassation a déjà eu l'occasion de préciser que : «le fait de se procurer pour soi-même ou pour autrui un avantage patrimonial frauduleux en manipulant des données informatiques de la manière précisée par cet article constitue un délit et n'est, dès lors, plus soumis à l'application de l'article 467, alinéa 1er du Code pénal» (Cass., 6 mai 2003, *Pas.*, 2003, p. 915; *Rev. dr. pén.*, 2004, p. 1168; *R.A.B.G.*, 2004, p. 637, note Y. Van Den Berghe). Cette hypothèse était explicitement visée par le législateur (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 15).

(131) Pour différents développements sur la notion de fraude informatique en droit français (où une disposition équivalente à l'art. 504*quater* de notre C. pén. avait été introduite dès 1988), voy. not. F. Chamoux, «La loi sur la fraude informatique : de nouvelles incriminations», *J.C.P.*, 1988, p. 3321; H. Croze, «L'apport du droit pénal à la théorie générale du droit de l'informatique – À propos de la loi n° 88-19 du 15 janvier 1988 relative à la fraude informatique», *J.C.P.*, 1988, p. 3333; J. Tappolet, «La fraude informatique», *Revue internationale de criminologie et de police technique*, 1988, pp. 351-357; M.-P. Lucas de Leyssac, «Fraude informatique : protection des systèmes de traitement automatisé de données, répression de la falsification de documents informatisés et mesures de prévention – Loi du 5 janvier 1988», *Droit et informatique*, 1988, pp. 18-26.

(132) C. Meunier, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 628.

(133) Celles-ci constituent les situations donnant lieu au plus grand nombre de plaintes en matière de criminalité informatique.

moyen d'une carte de paiement, la manipulation illicite des données relatives à un compte bancaire, l'accès à un parking payant ou réservé au moyen d'une fausse carte ou d'une carte détournée, les manipulations illégitimes effectuées par un employé de banque sur les comptes des clients en faveur de son propre compte (134) ...

Les éléments constitutifs de la fraude informatique présentant une certaine similitude avec ceux du faux informatique, et la fraude informatique s'appuyant souvent sur un faux, un même comportement infractionnel pourra, le cas échéant, donner lieu à des poursuites sur la base de ces deux préventions (135).

I. – *Éléments constitutifs*

30. La fraude informatique sur le plan matériel. Au niveau matériel, l'infraction suppose la mise en œuvre de moyens de recherche d'un avantage économique illégal par le biais de l'introduction, de la modification ou de l'effacement de données dans un système informatique ou de la modification de l'utilisation normale de ces données.

La définition de l'infraction repose donc sur la recherche d'un avantage économique illégal, et non sur son obtention (136). Il s'agit d'une infraction instantanée dont la prescription de l'action publique commence à courir à partir du moment de la mise en œuvre des moyens de recherche.

La première condition d'existence de l'infraction, et finalement la seule sur le plan matériel, consiste en une introduction, une modification ou une suppression de données dans un système informatique ou dans le recours à une technologie, quelle qu'elle soit, permettant de modifier l'usage normal de données stockées, traitées ou transmises par un système informatique. Cette condition se confondant avec celle du faux informatique, il est renvoyé à l'étude de cette infraction quant à la signification et à la portée de ces termes (137).

Sans une telle opération, il ne peut être question de fraude informatique. On relèvera que la disposition n'exige plus que l'avantage écono-

(134) Pour d'autres hypothèses de fraude informatique (envisagées avant l'adoption de la loi et donc formulées de façon générale), voy. not. B. Spruyt, «Computers op de strafbank. Analyse van het fenomeen informaticacriminaliteit : nationale en internationale strafrechtelijke perspectieven», *op. cit.*, pp. 272-275.

(135) En tant que tel, et sous réserve du respect des principes de légalité et de spécialité, cela ne pose pas de problème, dès lors que ces infractions viendront le plus généralement en concours.

(136) L'obtention de l'avantage n'étant plus une condition d'existence de l'infraction, il est indifférent que cet avantage ait été obtenu avant ou après la manipulation de données.

(137) *Cf. supra.*

mique illégal ait finalement été obtenu, de sorte que la fraude informatique est un délit de simple mise en danger (138) ou délit formel (139). Il faut, mais il suffit, que l'auteur ait opéré un traitement de données dont la partie poursuivante sera capable de prouver qu'il était en pouvoir causal avec l'avantage poursuivi. Cette condition a pour effet de soustraire à la répression l'acte qui ne présenterait aucun rapport de convenance avec le dessein incriminé. La définition de l'élément matériel de l'infraction recouvre donc, *in fine*, et sous la réserve déjà exprimée dans le cadre de l'analyse de la prévention de faux informatique quant à la précision des termes utilisés dans la définition (140), toute opération de traitement de données ou toute manipulation de données stockées dans un système informatique.

À l'origine, la définition de l'infraction n'était pas si large : la réalisation de la fraude informatique supposait, à l'instar de l'escroquerie visée à l'article 496 du Code pénal, que l'auteur ait obtenu un *avantage patrimonial frauduleux*. La réussite de son opération était donc une condition d'existence de l'infraction. À défaut pour le fraudeur de s'être procuré cet avantage, la prévention n'était pas établie mais constituait, le cas échéant, une simple tentative.

La disposition a été modifiée par la loi du 15 mai 2006 visant à mettre le texte belge en adéquation avec la Convention (141). Dorénavant, c'est la seule recherche de l'avantage économique illicite qui est sanctionnée (142).

Cette modification de la loi ne nous paraissait toutefois pas nécessaire, car le texte initial incriminait déjà la tentative de fraude informatique. Elle ne nous paraissait en outre pas très heureuse, car elle ouvrait très largement la définition matérielle de l'infraction, faisant ainsi dépendre essentiellement l'établissement de la prévention de la preuve de l'élément moral.

31. La fraude informatique sur le plan moral. La fraude informatique suppose que l'auteur ait été animé par un dol spécial, à savoir l'intention frauduleuse de se procurer ou de procurer à autrui un avantage économique illégal. Cet état d'esprit fait défaut si une personne

(138) Sur la notion de délit de mise en danger, voy. C. HENNAU et J. VERHAEGEN, *op. cit.*, p. 61.

(139) F. TULKENS et M. VAN DE KERCHOVE, *Introduction au droit pénal*, 6e éd., Diegem, Kluwer, 2003, p. 319.

(140) *Cf. supra.*

(141) *Cf. supra.*

(142) En ne soumettant plus la réalisation matérielle de l'infraction à l'obtention de l'avantage économique illicite poursuivi, le législateur a nettement distingué la fraude informatique de l'escroquerie de droit commun ou même de l'abus de confiance.

opère un retrait d'argent et dépasse involontairement le crédit de son compte ou le fait sciemment mais en étant convaincu d'y être habilité par les termes de son contrat d'ouverture de crédit (143).

Alors que le texte initial incriminait l'obtention d'un avantage patrimonial frauduleux, l'article 504*quater*, tel que modifié par la loi du 15 mai 2006, vise dorénavant la recherche, avec une intention frauduleuse, d'un avantage économique illégal. Cette notion d'avantage économique illégal n'a reçu aucun éclaircissement. Se différencie-t-elle de l'avantage patrimonial frauduleux? Il appartiendra au juge d'apprécier ce que cette notion recouvre. Qu'en sera-t-il, par exemple, de l'étudiant qui se serait introduit dans le système informatique de son établissement scolaire en vue de modifier les points obtenus à l'occasion d'un examen (144)? Serait-il susceptible d'en retirer un avantage économique illégal (145)? Et qu'en serait-il s'il modifiait les points d'un autre à la baisse? Il nous apparaît qu'en cette dernière hypothèse, l'agissement ne serait pas de nature à lui conférer un avantage économique. On relèvera qu'en tout état de cause, ces agissements, s'ils devaient échapper à la répression de l'article 504*quater* du Code pénal, relèveraient assurément des articles 550*bis* (*hacking* externe) et 550*ter* (sabotage de données) du même Code (*cf. infra*) (146).

II. – *Récidive*

32. Récidive spéciale, temporaire et obligatoire. Comme pour le faux informatique, la récidive prévue à l'article 504*quater*, §3, est spéciale, temporaire et obligatoire. Il est donc renvoyé à l'étude du faux informatique et aux développements qui y ont été faits à propos de la récidive (*cf. supra*).

La récidive est spéciale, à savoir qu'elle ne peut se fonder que sur une première condamnation pour des *infractions informatiques* visées

(143) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 628.

(144) S. EVRARD, «La loi du 28 novembre 2000 relative à la criminalité informatique», *op. cit.*, p. 242.

(145) C. MEUNIER considérait, sous l'empire de l'ancienne définition, que cette situation ne répondait pas à l'exigence d'un avantage patrimonial frauduleux («La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 628).

(146) Une question similaire se pose en ce qui concerne les *cookies* (*cf.* C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 629; F. DE VILLENFAGNE et S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A.&M.*, 2001, p. 70). Pour une approche technique du fonctionnement des *cookies*, voy. not. J.-M. DINANT, «Les traitements invisibles sur internet», in *Droit des technologies de l'information – Regards prospectifs*, Cahiers du C.R.I.D., n° 16, Bruxelles, Bruylant, 1999, p. 286.

aux articles 504*quater*, 210*bis* (faux informatique), 550*bis* (*hacking*) ou 550*ter* (sabotage informatique) ou que sur une condamnation basée sur les articles 259*bis* (prise de connaissance de (télé)communications privées) ou 314*bis* du Code pénal (infractions relatives au secret des (télé)communications privées).

Elle est par ailleurs temporaire, puisqu'elle n'est établie que pour autant que la seconde infraction ait été commise dans un délai de cinq ans à dater du prononcé de la première condamnation.

Elle est enfin obligatoire, puisque l'article 504*quater*, §3, prévoit que les peines de l'infraction comme de sa tentative seront doublées en cas de récidive (147). Le juge n'aura donc pas à apprécier l'opportunité de relever les seuils de peines.

III. – *Cas d'application*

33. Décisions de jurisprudence. Différentes décisions de jurisprudence ont été rendues en matière de fraude informatique, le plus souvent à la suite de retraits abusifs d'argent à des distributeurs automatiques (148) (avec une carte de banque volée, p. ex.), mais aussi pour des cas de *skimming* (149).

IV. – *Les peines*

34. Peines délictuelles. Les peines prévues par l'article 504*quater* du Code pénal sont un emprisonnement de six mois à cinq ans et/ou une amende allant de 26 à 100.000 EUR, de sorte que la fraude informatique est un délit. À titre de comparaison, les peines prévues par l'article 496 du Code pénal pour l'escroquerie sont un emprisonnement d'un mois à cinq ans et une amende de 26 EUR à 3.000 EUR. Le minimum de la peine privative de liberté et le maximum de l'amende sont donc plus élevés en cas de fraude informatique qu'en cas d'escroquerie de droit commun. On relèvera toutefois qu'en cas de condamnation du chef d'escroquerie, l'amende est obligatoire, alors qu'elle n'est que facultative en cas de fraude informatique. Sans doute cela se justifie-t-

(147) En l'absence de disposition plus précise, il convient de considérer que le doublement des peines s'applique tant aux minima qu'aux maxima.

(148) *Cf.* Cass., 6 mai 2003, *op. cit.*

(149) E. ROGER FRANCE, «La criminalité informatique», *op. cit.*, p. 115. Le *skimming* consiste à copier ou créer de toute pièce une carte bancaire (ou toute autre carte magnétique donnant accès à une valeur patrimoniale) au moyen d'un *skimmer* (lecteur-enregistreur de cartes magnétiques). Il est ainsi p. ex. possible de reformater une carte de fidélité d'un grand magasin en carte de crédit, rendant les recherches policières d'autant plus difficiles.

il par l'importance du risque économique que la fraude informatique est susceptible de faire peser sur le développement de l'économie numérique et des transactions électroniques.

Une peine de travail peut bien sûr être prononcée (150).

Les seuils de peines rendent par ailleurs possible la délivrance d'un mandat d'arrêt (151).

On notera encore qu'alors que l'article 496 du Code pénal relatif à l'escroquerie prévoit la possibilité d'assortir la peine d'une interdiction facultative des droits énumérés à l'article 31 du Code pénal, cette option n'a pas été retenue par le législateur lors de la rédaction de l'article 504*quater* du Code pénal.

Il est également à noter, à l'instar du faux informatique, que la fraude informatique n'a pas été reprise dans les infractions dont la condamnation pouvait être assortie d'une interdiction professionnelle sur la base de l'arrêté royal relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines fonctions, professions ou activités (152). Cela résulte probablement d'un oubli, dans la mesure où l'escroquerie (et la tentative d'escroquerie) est reprise parmi les infractions dont la condamnation peut être assortie d'une interdiction. Il apparaîtrait opportun, vu le développement des échanges financiers en ligne, de l'y insérer, puisque c'est sur la base de cet arrêté royal qu'il peut être fait interdiction à une personne d'exercer la profession d'agent de change, notamment.

Il convient encore de relever que l'excuse de parenté (exception à l'incrimination) prévue à l'article 462 du Code pénal est applicable à l'escroquerie mais ne l'est pas pour la fraude informatique. Il n'y a rien d'étonnant à cela, dans la mesure où, par définition, la fraude informatique n'implique pas qu'une personne ait été abusée, mais qu'un système informatique ait été sinon trompé, à tout le moins induit en erreur. Par ailleurs, l'exception à l'incrimination (ou cause d'excuse absolutoire, selon certains) prévue à l'article 462 du Code pénal tend à protéger l'intimité familiale et relationnelle d'une immixtion trop forte et non souhaitable des autorités judiciaires, alors que la fraude informatique n'opposera pas en principe des conjoints ou des apparentés au premier degré, mais plutôt des fraudeurs et des responsables de systèmes informatiques qui, la plupart du temps, ne se connaîtront pas.

(150) C. pén., art. 37*ter*, §1er, al. 2.

(151) L. 20 juillet 1990 relative à la détention préventive, art. 16, §1er, al. 1er.

(152) A.R. n° 22 du 24 octobre 1934 (*M.B.*, 27 octobre 1934).

Enfin, la personne qui se sera rendue coupable d'une fraude informatique fera obligatoirement l'objet de la confiscation spéciale des choses formant l'objet de l'infraction, de celles qui ont servi ou qui ont été destinées à les commettre, quand la propriété en appartient au condamné, ainsi que des choses qui ont été produites par l'infraction (153). Cette même personne pourra faire l'objet d'une confiscation spéciale facultative des avantages patrimoniaux tirés directement de l'infraction, des biens et des valeurs qui y auront été substitués ainsi que des revenus de ces avantages investis (154).

V. – *Questions spécifiques de droit pénal*

A. *Tentative de fraude informatique*

35. Incrimination de la tentative de fraude informatique. La tentative du délit est incriminée à l'article 504*quater*, §2, qui prévoit une peine allant de 6 mois à 3 ans d'emprisonnement et/ou une amende comprise entre 26 et 50.000 EUR. Ce taux de peine permet la délivrance d'un mandat d'arrêt (155).

36. Faible incidence pratique de l'incrimination de la tentative. Les cas dans lesquels la seule tentative sera incriminée seront limités aux situations dans lesquelles le délinquant aura été interpellé alors qu'il avait rassemblé tous les éléments nécessaires à l'exercice d'une fraude informatique et mis en œuvre les moyens tendant à sa réalisation mais n'avait pas encore entamé l'exécution de celle-ci par l'introduction, la modification ou la suppression de données dans un système informatique. En effet, en ce dernier cas, compte tenu du fait que l'infraction de fraude informatique elle-même porte précisément sur l'activité de recherche d'un avantage économique illégal par l'introduction, la modification ou la suppression de données dans un système informatique et ce, indépendamment de tout résultat, il nous apparaît qu'il ne s'agira plus d'une tentative mais d'une fraude informatique entièrement réalisée. En d'autres termes, dès que l'auteur aura posé les premiers actes d'exécution de l'infraction par l'introduction, la modification ou la suppression de données dans un système informatique, il aura, de fait, réalisé entièrement l'infraction. La tentative ne portera donc, le plus souvent,

(153) C. pén., art. 42, 1° et 2°, et 43.
(154) C. pén., art. 42, 3°, et 43*bis*.
(155) L. 20 juillet 1990 relative à la détention préventive, art. 16, §1er, al. 1er.

que sur les actes d'exécution préalables à l'introduction, la modification ou la suppression de données dans un système informatique.

La manœuvre consistant à se procurer un *skimmer* (programmateur de cartes magnétiques), des cartes magnétiques vierges (appelées *white cards* ou *yes cards*) ainsi que des numéros de cartes de crédit réelles pourrait ainsi constituer une tentative de fraude informatique si le juge était amené à considérer que l'ensemble de ces opérations répondait à l'exigence de l'univocité circonstancielle (156). Tel serait le cas si, après avoir replacé l'acte qui lui est soumis dans son *iter criminis* et après l'avoir envisagé dans sa matérialité et sa subjectivité, le juge considérait, à l'issue de ce double examen, qu'il n'y a pas d'équivoque dans le comportement de l'auteur, c'est-à-dire que ce comportement ne pourrait s'expliquer autrement que par la volonté de celui-ci de commettre une fraude informatique. Il pourra alors conclure à l'existence d'un commencement d'exécution. *A contrario*, la seule possession d'un *skimmer* et de cartes vierges ne pourrait être incriminée s'il apparaissait que ces ustensiles étaient d'usage licite pour leur possesseur (p. ex., pour l'établissement de cartes d'accès à une bibliothèque ou de cartes de fidélité).

VI. – *Questions particulières de procédure pénale*

37. Écoutes de télécommunications privées. Il convient de noter que la fraude informatique a été intégrée dans la liste des infractions susceptibles de donner lieu à la mise en œuvre d'écoutes téléphoniques (157).

§ 3. – Accès non autorisé à un système informatique (*hacking*) et infractions voisines (C. pén., art. 550*bis*)

38. Notion. Le *hacking*, ou accès non autorisé dans un système informatique, a été introduit dans le Code pénal, à l'article 550*bis*, par la loi du 28 novembre 2000. Avant l'adoption de cette disposition, seules quelques lois éparses sanctionnaient certains agissements assimilables à du *hacking* (158). Sous réserve de celles-ci, l'accès illicite à un système

(156) J. Constant, *Traité élémentaire de droit pénal*, t. I, Liège, Imprimeries nationales, 1965, pp. 261-262.
(157) C. instr. crim., art. 90*ter*, §2, 10°*ter*.
(158) Les art. 61, 6°, et 63, 8°, de la loi sur la Banque-Carrefour de la sécurité sociale ou les dispositions de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel permettaient d'appréhender certains comportements. Plus indirectement, c'est sur pied de l'art. 114, §8, de la loi Belgacom de 1991 que différents «*hackers*» ont été condamnés (voy. not. Corr. Gand,

informatique ne constituait pas, en soi, une infraction spécifique sanctionnée pénalement (159).

Par l'adoption de cette disposition (et des autres dispositions du Titre IX du Code pénal), le législateur a entendu consacrer la protection pénale d'une valeur nouvelle, à savoir la sauvegarde de la confiance du public dans le fonctionnement de l'outil informatique, mais aussi la confidentialité des données informatiques.

En substance, le *hacking* peut être défini comme étant le fait de s'introduire dans le système informatique d'autrui à son insu, sans disposer de l'habilitation nécessaire à cette fin.

39. Distinction *hacking* interne – *hacking* externe. La disposition distingue le *hacking* interne, qui a été le fait d'un individu disposant déjà d'un droit d'accès sur le système informatique visé et qui aurait excédé les limites de son autorisation, du *hacking* externe, qui est celui réalisé par une personne étrangère au système pris pour cible.

La raison pour laquelle le législateur a entendu distinguer le *hacking* interne du *hacking* externe réside dans le fait que l'accès illégal à certaines parties d'un réseau sera constaté plus fréquemment au sein d'une organisation du fait des facteurs les plus divers (contacts personnels, structure du réseau, environnement de travail ...) et qu'il existe d'autres voies que le droit pénal pour sanctionner le *hacker* interne qui aurait agi sans intention de nuire ou sans but de lucre (et notamment le droit du travail, le droit disciplinaire, le droit civil ...) (160).

Le Conseil d'État avait critiqué cette différence de traitement (161), considérant qu'elle n'avait pas lieu d'être, mais elle a été validée par la Cour constitutionnelle, qui, par un arrêt du 24 mars 2004, a décidé que l'article 550*bis* du Code pénal ne violait pas les articles 10 et 11 de la Constitution en ce qu'il exige de la part du *hacker* interne qu'il ait été animé par le dol spécial alors que ce même article se satisfait du simple dol général pour le *hacker* externe (162).

11 décembre 2001, *Computerr.*, 2001, p. 84, note E. KINDT et E. SZAFRAN; *A. & M.*, 2001, p. 157, note B. MICHAUX; *T. Strafr.*, 2001, p. 97, note B. MICHAUX et S. EVRARD; Corr. Louvain, 28 février 2000, *A.J.T.*, 1999-2000, p. 885, avec note G.-L. BALLON, «Misbruik van andermans computersysteem om gratis internet te kunnen bezoeken»).

(159) C'est en se sens que le Tribunal correctionnel de Bruxelles avait tranché dans le cadre de l'affaire *BISTel* (*cf. supra*).

(160) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 16.

(161) Avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 17.

(162) C. const., 24 mars 2004, n° 51/2004, *Arr. C.A.*, 2004, p. 619. La Cour a considéré que la distinction étant basée sur le pouvoir d'accès au système informatique, il s'agissait là d'un critère objectif justifiant une différence de traitement.

I. – Hacking *externe*

A. *Éléments constitutifs*

40. Définition. Aux termes de l'article 550*bis*, §1er, du Code pénal, «celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement».

41. Le *hacking* externe sur le plan matériel. Les éléments constitutifs du *hacking* externe sont, sur le plan matériel, un accès ou un maintien dans un système informatique, même non sécurisé, alors que celui qui s'y trouve ne disposait d'aucune autorisation, même partielle, d'y accéder ou de s'y maintenir.

42. Absence totale d'autorisation. L'absence totale d'autorisation d'accès ou de maintien dans le système de traitement automatisé de données constitue le premier élément matériel de l'infraction. Cet élément n'a pas fait l'objet de développements particuliers lors des travaux préparatoires. La notion d'autorisation n'a pas été précisée. Il convient donc de l'entendre dans le sens usuel que lui prête le langage courant (163), à savoir le droit ou la permission, concédé par une personne habilitée à ce faire, d'accéder ou de se maintenir dans le système informatique concerné. Cette autorisation peut être expresse autant que tacite (164). Il revient à la partie poursuivante d'établir, le cas échéant, l'absence d'autorisation, même si la preuve d'un élément négatif peut s'avérer difficile. On imagine en effet les difficultés auxquelles se trouveront confrontées les autorités chargées des poursuites lorsqu'elles auront à établir la preuve d'un *hacking* commis à l'égard d'un système informatique non sécurisé, surtout lorsque celui-ci sera interconnecté à d'autres systèmes d'accès libre (165).

Cette condition matérielle d'absence d'autorisation se distingue de la condition morale, même si le dol sera plus facile à prouver lorsqu'il aura été préalablement établi que l'auteur ne disposait pas de l'autorisation requise pour accéder ou se maintenir dans le système visité. Ainsi

(163) Il appartiendra au juge d'apprécier l'existence ou non d'une autorisation. Nous reviendrons sur cette notion dans le cadre du *hacking* interne.

(164) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 633.

(165) Les réseaux interconnectés n'étant pas délimités physiquement, il peut s'avérer malaisé de déterminer que l'utilisateur était dépourvu d'autorisation d'accès pour pénétrer une partie du système et qu'il avait conscience d'avoir excédé les limites de son autorisation.

en sera-t-il, par exemple, de l'employé licencié ou dont le contrat serait venu à échéance et qui continuerait, alors qu'il n'y serait plus autorisé, à se connecter au système informatique de son ancien employeur pour accéder à l'internet (166).

43. Infraction réalisée alors même que le *hacking* n'aurait occasionné aucun dommage. Le *hacking* externe est un délit de mise en danger ou délit formel, qui se réalise indépendamment du résultat dommageable qu'il est susceptible de causer (167), le dommage occasionné à la suite d'un *hacking* ne constituant qu'une circonstance aggravante (*cf. infra*) et non un élément constitutif de l'infraction. La simple consultation du contenu du disque dur d'un système informatique n'entraînant aucun préjudice suffit donc à la répression (168).

L'effraction d'un système de sécurité n'a pas non plus été retenue comme élément constitutif de l'infraction (169). Il ne faut donc pas que le *hacker* ait fait un usage frauduleux d'un code d'accès ou ait contourné d'une quelconque manière un mécanisme d'identification ou de

(166) Dans ce cas d'espèce, le *hacking* externe serait aggravé par l'intention frauduleuse (art. 550*bis*, §1er, 2°) ainsi que par l'usage du système informatique (art. 550*bis*, §3, 2°).

(167) Le Conseil d'État s'était inquiété du fait que «dans un contexte informatique, la simple curiosité peut susciter un délit pénal» (Avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 17). Mais le législateur avait estimé que «l'intérêt juridique protégé par les nouvelles dispositions était en premier lieu l'intégrité du système» (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 17) et que ne pas punir ceux qui agiraient contre ces systèmes, même sans intention frauduleuse ou méchante, «ouvrirait la voie à toutes sortes d'abus qui mettraient en danger la sécurité des systèmes informatiques» (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/010).

(168) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 632.

(169) Contrairement à ce qui a été décidé dans d'autres pays, et notamment aux Pays-Bas, où l'infraction de *hacking* n'est établie que s'il y a eu viol d'un système de sécurité avec intention de nuire. On notera par ailleurs qu'en France, l'art. 323-1 du C. pén. soumet le *hacking* à un dol spécial : le *hacker* n'est punissable que s'il a accédé ou s'est maintenu frauduleusement dans tout ou partie d'un système de traitement de données. De plus, cette même disposition limite le *hacking* aux cas où il est résulté de l'intrusion une suppression ou une modification des données contenues dans le système ou une altération du fonctionnement de ce système. Un internaute avait ainsi constaté une faille sur le site de la chaîne de distribution TATI. Il était parvenu à accéder au serveur de la chaîne puis à télécharger le fichier client. Il avait par la suite averti les responsables du site et publié plusieurs articles sur le sujet. TATI avait porté plainte pour accès et maintien frauduleux dans un système automatisé de données et pour vol de base de données. En première instance, il avait été condamné à 1.000 EUR d'amende avec sursis. Sur appel du ministère public, la Cour d'appel de Paris l'avait acquitté, considérant que pour qu'il y ait accès ou maintien frauduleux, son exploitant devait avoir indiqué le caractère confidentiel des données ou avoir pris des mesures destinées à les protéger (condition que la loi belge ne prévoit pas). La Cour avait conclu à l'absence d'élément intentionnel (Paris, 12e ch., 30 octobre 2002, *Expertises*, 2003, n° 266, p. 36, note C. MOREL, «Pas d'accès frauduleux sans sécurité : l'application au responsable d'un site web de l'adage *nemo auditur propriam suam turpitudinem allegans* en matière de fraude informatique»). De façon plus générale, le Comité européen pour les problèmes criminels avait relevé qu'il y avait peu de pays dont la législation permettait de sanctionner un comportement consistant purement et simplement dans l'accès non autorisé à un réseau informatique (*Rapport du Comité européen pour les problèmes criminels*, pp. 54-56).

cryptage (170). La raison en est, selon le législateur, que cela aurait causé de trop nombreuses difficultés pour la définition de l'infraction (et du niveau de protection requis) et que cette condition serait probablement rapidement devenue sans objet dans la mesure où les protections de systèmes informatiques sont devenues de plus en plus standards (171). Bien entendu, si la protection du système n'est pas une condition requise pour la mise en œuvre de l'article 550*bis*, la démonstration de la violation d'un tel système facilite à l'évidence la démonstration du caractère interdit de l'accès (172).

44. Notions d'accès et de maintien. L'infraction se caractérise ensuite par un accès ou un maintien dans un système informatique (173). Ces notions d'accès ou de maintien ne sont pas définies. Elles devront donc être appréciées par le juge. L'accès n'étant pas lié à l'emploi d'une technique d'intrusion particulière, il devra être entendu de façon large. On notera d'ailleurs que la loi n'exige pas que l'accès ou le maintien ait donné lieu à l'introduction, la modification ou la suppression de données dans le système informatique visité. Cette disposition permet donc de sanctionner la prise de connaissance du contenu de courriers électroniques stockés dans la messagerie d'un tiers ou de SMS ou fichiers enregistrés dans la mémoire d'un GSM. Selon C. Meunier, la simple auscultation du contenu crypté ou non apparaissant sur l'écran d'un ordinateur privé allumé relève déjà de l'article 550*bis* du Code pénal (174). Nous ne partageons pas ce point de vue. Il nous apparaît en effet que la notion d'accès, certes imprécise, suppose néanmoins un acte positif (*modus operis*) traduisant avec certitude la volonté de l'agent de pénétrer d'une quelconque façon dans le système informatique convoité. Cette démarche d'intrusion ne saurait, à notre estime, se satisfaire d'un seul regard. À défaut, et à suivre une interprétation large de la

(170) Si l'infraction de *hacking* devait être rapprochée d'une prévention sanctionnant un comportement similaire adopté dans le monde physique, sans doute s'agirait-il de la violation de domicile, visée à l'art. 439 du C. pén. Les intérêts protégés étant différents, la comparaison n'offre qu'un intérêt limité. Toutefois, on relèvera que l'art. 439 du C. pén. ne sanctionne la violation de domicile que lorsqu'elle a été commise avec violences, menaces ou effraction ou lorsqu'elle a été faite la nuit.

(171) *Doc. parl.*, Chambre, sess. ord., 1999-2000, n° 50 0213/001, p. 17. Voy. sur cette question, P. VAN EECKE, *Criminaliteit in cyberspace : misdrijven, hun opsporing en vervolging op de informatiesnelweg*, *op. cit.*, p. 25.

(172) Ch. FERAL-SCHUHL, *Cyberdroit – Le droit à l'épreuve de l'Internet*, 3e éd., Paris, Dalloz, 2002, p. 46.

(173) Comme le soulignent F. DE VILLENFAGNE et S. DUSOLLIER, le maintien est la suite logique de l'accès de sorte qu'un accès peut être licite mais le maintien peut être illicite (F. DE VILLENFAGNE et S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A.&M.*, 2001, p. 73).

(174) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 632.

notion d'accès, le seul coup d'œil volontaire sur l'écran du voisin tomberait sous le coup de l'article 550*bis*, ce qui, assurément, ne correspond pas à l'esprit de la disposition. Il en irait, selon nous, autrement du curieux qui ne se limiterait pas à regarder ce qui apparaît sur l'écran de l'ordinateur d'autrui et ferait, par exemple, usage de la souris pour ouvrir une fenêtre qui avait été réduite ou pour faire défiler un texte.

L'incrimination du maintien, indépendamment de l'accès, vise à sanctionner l'auteur qui aurait accédé de bonne foi et par inadvertance à un système informatique sans disposer de l'autorisation nécessaire puis se serait maintenu dans ledit système après avoir eu conscience du caractère illicite de l'intrusion. Elle vise également à sanctionner l'agent qui, bien que disposant de l'autorisation d'accès nécessaire, aurait épuisé ou excédé son autorisation en restant pour une durée supérieure à la durée autorisée ou en accédant à une partie du système à laquelle il n'est pas autorisé à accéder. Cette distinction entre l'accès et le maintien n'est pas dépourvue d'incidences pratiques, notamment en matière de prescription, puisque l'accès est une infraction instantanée, tandis que le maintien est une infraction continue (175).

On rappellera encore que la notion de système informatique visée dans la disposition dépasse largement celle d'ordinateur personnel et que l'infraction pourra donc être exécutée à l'égard d'autres formes de systèmes informatiques (un agenda électronique, un GSM, un récepteur GPS, un terminal de paiement électronique, voire même une simple carte à puce ...).

Par ailleurs, l'incrimination de l'accès ou de maintien dans un système informatique est indépendante d'autres incriminations relatives à la prise de connaissance de données. En d'autres termes, la prise de connaissance de données opérée à la suite d'un *hacking* peut être punie sur la base de l'article 550*bis* du Code pénal mais également, le cas échéant, sur pied d'autres dispositions pénales (176). Ainsi, l'accès illicite à des données à caractère personnel (au sens de la loi du 8 décembre 1992) ensuite d'un *hacking* pourrait donner lieu à des poursuites conjointes. On pense également aux articles 259*bis* et 314*bis* du Code pénal, qui concernent l'interception de télécommunications pendant leur transmission, ainsi qu'à l'article 458 du Code pénal, relatif au secret professionnel.

(175) *Ibid.*, p. 633.

(176) Les travaux préparatoires le précisent explicitement : «Sans préjudice de cette disposition, les dispositions pénales d'autres régimes de protection concernant des catégories particulières de données restent d'application. En effet, la philosophie à la base du projet repose sur l'idée que lorsque certaines informations justifient une protection spéciale du fait même de leur nature, il y a lieu de prévoir un régime de protection séparé : le fait que ces informations soient consignées sur papier ou sur un support informatique est non pertinent à cet égard» (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 17).

45. Le *hacking* externe sur le plan moral. Sur le plan de l'élément moral, la loi exige, dans le chef de l'auteur, qu'il ait été animé par le dol général. Il faut donc, mais il suffit, qu'il soit démontré qu'il a agi avec connaissance effective et volonté ou, à tout le moins, acceptation de commettre l'infraction (177). Les manipulations malheureuses, la maladresse ou la maîtrise insuffisante de l'outil informatique ne peuvent donc conduire à un *hacking*. La preuve du dol sera sans doute difficile à établir en cas de *hacking* commis par l'intermédiaire de réseaux interconnectés puisque, ceux-ci n'étant pas délimités physiquement, il peut s'avérer malaisé pour l'utilisateur de réaliser qu'il a excédé les limites du réseau auquel il était autorisé à accéder.

Contrairement au faux informatique, à la fraude informatique ou au *hacking* interne, l'intention frauduleuse ou le dessein de nuire ne sont pas requis (178). Selon les travaux préparatoires de la loi, il en va ainsi parce que l'intrusion de tiers étrangers au système informatique met en danger la sécurité du réseau lui-même (179).

46. L'intention frauduleuse comme circonstance aggravante. L'intention frauduleuse sera toutefois constitutive d'une circonstance aggravante. L'article 550*bis*, §1er, alinéa 2, du Code pénal prévoit en effet qu'en pareilles circonstances, la peine du *hacking* externe sera comprise entre un an et deux ans d'emprisonnement et que l'amende sera comprise entre 26 et 25.000 EUR. Ainsi en irait-il, par exemple, de l'informaticien licencié qui s'introduirait dans le système informatique de la société l'ayant remercié afin d'y voler des fichiers ou des programmes (180).

(177) Pour un cas d'application où la question de l'intentionnalité de l'auteur a été débattue, voy. not. Corr. Hasselt, 21 janvier 2004, *Computerr.*, 2004, pp. 21 et s.

(178) On relèvera que le Sénat avait amendé le projet de loi en prévoyant un dol spécial dans le chef du *hacker* externe. Mais la Chambre avait rejeté cet amendement, considérant qu'il n'était pas acceptable que le *hacking* se limitant à la violation d'un système informatique (pour tester un système de sécurité, par exemple) échappe à la répression, le *hacking* devant être considéré comme un délit de mise en danger en tant que tel, quels que soient les intentions malveillantes particulières ou les effets atteints (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 17).

(179) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 16.

(180) Il y aurait en cette hypothèse une autre circonstance aggravante, soit la reprise des données (*cf. infra*).

B. *Peine*

47. Peines délictuelles. La peine du *hacking* externe est un emprisonnement de trois mois à un an et une amende comprise entre 26 et 25.000 EUR, ce qui rend possible la délivrance d'un mandat d'arrêt (181).

Une peine de travail peut être prononcée (182).

C. *Illustrations*

48. Exemples de *hackings* externes. À titre d'illustrations de *hackings* externes, citons le fait pour une personne de pénétrer le réseau fermé d'une entreprise par le biais de l'infrastructure publique de télécommunications (183) ou le fait de parasiter une connexion *wi-fi* (184), même non sécurisée. On peut encore relever, avec C. Meunier, le fait de s'introduire dans le système informatique d'une société en vue de démontrer la fragilité de son système de sécurité ou le simple visionnage des fichiers stockés sur l'appareil photo numérique ou la caméra digitale d'un tiers (185).

II. – Hacking *interne*

A. *Éléments constitutifs*

49. Notion. Aux termes de l'article 550*bis*, §2, du Code pénal : «celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement».

Les éléments constitutifs du *hacking* interne sont donc quelque peu différents de ceux du *hacking* externe, puisque le §2 punit celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique.

(181) L. 20 juillet 1990 relative à la détention préventive, art. 16, §1er, al. 1er.
(182) C. pén., art. 37*ter*, §1er, al. 2.
(183) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/004, p. 6.
(184) C'est-à-dire une connexion sans fil. En ce cas, il y aura lieu de retenir également la circonstance aggravante visée au §3, 2°, de l'art. 550*bis*. Ce comportement pourrait également tomber sous le coup de l'art. 145, §3, 1°, de la loi du 13 juin 2005 relative aux communications électroniques (*cf. infra*).
(185) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 635.

50. Le *hacking* interne sur le plan matériel. Le *hacking* interne suppose, comme élément matériel, que le *hacker* ait disposé, préalablement à la commission de l'infraction, d'un droit d'accès partiel au système informatique et qu'il ait outrepassé son pouvoir d'accès pour pénétrer ou se maintenir dans une partie du système informatique à laquelle il n'était pas ou plus autorisé à accéder. Cette autorisation est un élément constitutif de l'infraction. C'est précisément ce qui distingue, sur le plan matériel, le *hacking* interne du *hacking* externe. Comme souligné *supra*, la loi ne définit pas la notion d'autorisation. Elle ne précise pas s'il doit s'agir d'une autorisation *géographique* (liée aux portions du système informatique librement accessibles à l'utilisateur), *fonctionnelle* (se rapportant aux opérations que l'utilisateur peut effectuer) ou temporaire (pour une période limitée) (186). En l'absence de précision, il nous apparaît que ces différentes formes d'autorisations correspondent à la notion visée à la disposition. La notion d'autorisation n'implique d'ailleurs pas l'existence d'un rapport contractuel ou hiérarchique entre le donneur d'autorisation et le bénéficiaire. Le *hacking* interne ne se limite donc pas aux seuls cas de *hackings* commis par des employés à l'encontre du système informatique de leur employeur.

Tout comme le *hacking* externe, le dépassement du pouvoir d'accès suppose que l'auteur accède à un système informatique. Et, comme le souligne C. Meunier, bien que le maintien dans un système informatique ne soit pas expressément visé par la disposition, la cohérence de l'article 550*bis* recommande d'y étendre celui-ci lorsque ledit maintien est la continuation d'un accès non autorisé au système informatique (187).

51. Infraction réalisée alors même que le *hacking* n'aurait occasionné aucun dommage. Comme pour le *hacking* externe, la loi n'exige pas, au rang des conditions matérielles de l'infraction, qu'un dommage ait été causé. Il s'agit seulement d'une circonstance aggravante (*cf. infra*).

À titre d'illustration, citons la situation de l'étudiant disposant d'un droit d'accès partiel au serveur de son établissement et profitant de celui-ci pour aller prendre connaissance de questions d'examens hébergées sur une partie du serveur à laquelle il n'est pas autorisé à accéder.

(186) Sur ce dernier point, en droit français, voy. not. G. HAAS, «Les limites de la répression de la fraude informatique – Pour une politique de sécurité des systèmes d'information», *Expertises*, juin 2006, pp. 233-234.
(187) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 636.

Citons encore le cas de la consultation de fichiers stockés sur un système informatique d'un employé par un de ses supérieurs alors même que ce dernier n'aurait pas accès auxdits fichiers.

52. Le *hacking* interne sur le plan moral. Au niveau de l'élément moral, le *hacking* interne suppose, à la différence du *hacking* externe, que l'auteur ait agi avec un dol spécial, soit l'intention frauduleuse (appât du gain illicite) ou le but de nuire (malveillance), de sorte que le niveau d'incrimination s'en trouve élevé d'autant (188). Il en découle que le seul accès ou maintien illicite involontaire ou en connaissance de cause dans un système informatique en dépassement du pouvoir d'accès ne constitue pas un *hacking* interne et n'expose donc pas son auteur à la sanction pénale (189). Toutefois, si cet accès ou ce maintien a causé des dommages, le comportement devient répréhensible sur la base de l'article 550*ter* du Code pénal.

Comme indiqué ci-avant, cette différence de traitement entre le *hacker* interne et le *hacker* externe avait été soumise à la Cour constitutionnelle, laquelle avait considéré qu'il n'y avait pas de discrimination au sens des articles 10 et 11 de la Constitution.

B. *Peines*

53. Peines délictuelles. La peine du *hacking* interne doit être comprise entre six mois et deux ans d'emprisonnement (soit le double du *hacking* externe) et l'amende peut aller de 26 à 25.000 EUR. Le juge peut également prononcer une peine de travail autonome comprise entre quarante-six et trois cents heures (190). Un mandat d'arrêt peut être décerné à l'égard du *hacker* interne (191).

III. – *Circonstances aggravantes*

54. Circonstances aggravantes communes. La loi a institué trois circonstances aggravantes communes aux deux types de *hacking*, à savoir la reprise de données, l'utilisation du système *hacké* et le dommage causé à celui-ci.

(188) En ce qui concerne ces notions, il est renvoyé aux développements qui y ont été consacrés dans le cadre de l'étude du faux informatique.

(189) Il n'en demeure pas moins que ce comportement pourrait entraîner, le cas échéant, d'autres formes de sanctions (disciplinaire, civile ...).

(190) C. pén., art. 37*ter*, § 1er, al. 2.

(191) L. 20 juillet 1990 relative à la détention préventive, art. 16, § 1er, al. 1er.

Lorsqu'une seule ou plusieurs de ces circonstances aggravantes seront rencontrées, la peine sera portée à un an à trois ans d'emprisonnement et/ou 26 à 50.000 EUR d'amende.

55. Reprise de données. La première circonstance aggravante concerne la reprise de données ou le vol de données (art. 550*bis*, § 3, 1°). Elle vise la soustraction, en original ou en copie, de données extraites à la suite d'un *hacking*, mais aussi la simple prise de connaissance de ces données. Elle ne vise pas la soustraction d'un support de données (192).

En insérant cette circonstance aggravante dans le Code pénal, la loi a mis un terme à la controverse relative au vol de données sous l'emprise des articles 461 et suivants du Code pénal (193).

Les termes de la loi étant très généraux, la reprise peut certainement être faite par la copie des données sur un support de mémoire quel qu'il soit (CD-Rom, disquette, DVD, clé USB ...), mais encore, par exemple, par la photographie de l'écran sur lequel apparaissent les données auxquelles le *hacking* a permis d'accéder (194).

Dans les travaux préparatoires, le vol de secrets d'entreprises dans le cadre de l'espionnage industriel et la prise de connaissance de données informatiques sont donnés en exemple (195). Il nous semble toutefois que ce dernier exemple prête à confusion. La circonstance aggravante vise en effet l'appropriation de données par le biais d'un enregistrement ou d'une copie réalisée à la suite d'un *hacking*. La simple prise de connaissance de données stockées dans un système informatique ne nous

(192) Le fait d'emporter des données informatiques imprimées ou stockées sur un support ne constitue pas un vol de données, mais, le cas échéant, un vol du support lui-même (voy. Th. VERBIEST et E. WÉRY, *Le droit de l'internet et de la société de l'information. Droits européen, belge et français*, *op. cit.*, p. 20).

(193) Une partie de la jurisprudence considérait en effet, avant l'entrée en vigueur de la loi, que la qualification de vol, de même que celle d'abus de confiance, ne pouvaient s'appliquer à des données informatiques dès lors que celles-ci étaient dépourvues de caractère physique et ne pouvaient faire l'objet d'une soustraction ou d'un détournement. Cette jurisprudence soulignait par ailleurs qu'en pareils cas, le propriétaire des données *volées* ne se trouvait pas dépossédé une fois la copie réalisée (Liège, 25 avril 1991, *Rev. dr. pén.*, 1991, p. 1013; Corr. Verviers, 4 octobre 1989, *J.L.M.B.*, 1990, p. 709; Corr. Malines, 16 février 2006, *Nullum Crimen*, 2007, p. 161). Une autre partie de la jurisprudence considérait que les qualifications de vol et d'abus de confiance pouvaient être retenues (voy. à ce propos, E. ROGER FRANCE, «La criminalité informatique», *op. cit.*, p. 120, note 64). Voy. égal. J.-P. SPREUTELS, «Le vol de données informatiques», *Rev. dr. pén.*, 1991, p. 1027.

(194) Sur ce dernier point, C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 639.

(195) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 6. Comme le souligne C. MEUNIER, si le vol de données est opéré par un employé au détriment de son entreprise et que ces données sont communiquées à des tiers, cet employé pourrait devoir répondre également de l'art. 309 du C. pén. («La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 638).

paraît pas relever de cette circonstance aggravante, mais de la seule prévention de *hacking*. Comme déjà indiqué, cette attitude est en effet sanctionnée par les §§ 1er et 2 de l'article 550*bis*, puisque la disposition entend protéger l'intégrité des systèmes informatiques autant que la confidentialité des données qui y sont stockées.

Au niveau de l'élément moral, la loi ne précisant rien, il nous apparaît que la circonstance aggravante ne sortira ses effets que pour autant que l'auteur ait été animé du dol général, à savoir l'intention de reprendre les données. Cela se déduit des termes de la disposition, la notion de «reprise» impliquant, à notre estime, une démarche certainement volontaire. Cela a pour conséquence que l'enregistrement des données dans les fichiers temporaires du système informatique utilisé par l'agent pour commettre le *hacking* ne suffira pas nécessairement à établir qu'il y a bien eu reprise des données. Il faudra encore que la partie poursuivante prouve que cet enregistrement était volontaire (p. ex., parce que structuré et planifié) et non seulement automatique et routinier.

On relèvera encore que l'application de l'article 550*bis* et de ses circonstances aggravantes n'empêche pas l'application conjointe de la loi du 30 juin 1994 concernant la protection juridique des programmes d'ordinateur (196). Selon les articles 1er et 2 de cette loi, les programmes d'ordinateur, en ce compris le matériel de conception préparatoire, sont protégés par le droit d'auteur s'ils sont originaux, en ce sens qu'ils sont une création intellectuelle propre à leurs auteurs. Une peine d'amende de 100 à 100.000 EUR peut être infligée à charge des distributeurs de programmes contrefaits mais également des détenteurs de mauvaise foi des copies illicites.

56. Utilisation du système visité. La deuxième circonstance aggravante est relative à l'utilisation du système d'autrui (art. 550*bis*, §3, 2°). Elle vise notamment le fait d'utiliser le système informatique visité pour s'en servir comme base relais en vue *d'attaquer* un autre ordinateur, mais également le vol de temps ou de bande passante (197). En raison de la largesse des termes utilisés, elle vise encore le seul usage des capacités de traitement du système informatique *hacké*. Or, dans bien des cas (198), l'accès ou le maintien dans un système informatique ne sera possible que moyennant l'exécution d'opérations sur ce système. Sans doute, dans ces cas-là, l'usage sera-t-il donc souvent de mise après un *hacking*, de sorte qu'en pareille hypothèse, le *hacker* externe risquera finalement la même peine que le *hacker* interne (199). On tempérera cependant cette observation par le fait que, bien que la loi ne précise rien de particulier quant à l'élément moral, le libellé de la circonstance aggravante nous semble indiquer que la conséquence visée doit être volontaire pour être prise en compte. Il semble donc que le dol général soit nécessaire à la répression et que l'auteur ait volontairement et en connaissance de cause fait un usage du système visité.

(196) L. 30 juin 1994 relative au droit d'auteur et aux droits voisins (*M.B.*, 22 novembre 1994) et L. 30 juin 1994 transposant en droit belge la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur (*M.B.*, 27 juillet 1994).

(197) L'abus de connexion *wi-fi* relève de cette circonstance aggravante. Le législateur cite comme exemple l'utilisation de la capacité du système entraînant une limitation temporaire des possibilités des autres utilisateurs (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001 et 0214/001, p. 17).

(198) On vise ici les cas de *hackings* réalisés par la voie de l'introduction, la modification ou la suppression de données dans un système informatique.

57. Dommage au système informatique ou aux données. La troisième circonstance aggravante est relative au fait de causer un dommage, même non intentionnellement, au système informatique visité ou aux données qui y sont stockées, traitées ou transmises (art. 550*bis*, §3, 3°) (200). Cela concerne tant le dommage volontaire qu'involontaire. Au niveau moral, il sera donc indifférent que l'auteur ait été animé du dol ou ait commis une simple faute. On notera toutefois que le sabotage intentionnel est puni plus sévèrement par ailleurs (*cf. infra*, C. pén., art. 550*ter*) (201).

On notera encore que la circonstance aggravante vise tout type de dommage, qu'il soit matériel ou immatériel, causé au système visité ou aux données qui y sont stockées. Tombent donc sous le coup de cette incrimination, le seul ralentissement de fonctionnement du système informatique visité (202) (pour autant, bien entendu, qu'il soit établi que ce ralentissement a causé un préjudice) comme la détérioration physique du système ou d'un de ses périphériques.

(199) F. DE VILLENFAGNE, S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A.&M.*, 2001, p. 68; C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 639.

(200) On notera avec H. GRAUX que les frais engagés pour assurer la protection d'un système informatique ne font pas partie, en tant que tel, du dommage dont la partie civile, victime de *hacking*, peut prétendre au remboursement à l'encontre de l'auteur de l'infraction (H. GRAUX, note sous Corr. Eupen, 15 décembre 2003 et Corr. Hasselt, 21 janvier 2004, *Computerr.*, 2004, pp. 131-133). Il s'agit en effet d'une conséquence de l'obligation générale de protection des données s'imposant à l'exploitant d'un système informatique contenant des données sensibles. Cette obligation trouve notamment son fondement dans l'art. 16, §4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (*M.B.*, 18 mars 1993), puisque cette disposition impose au responsable du traitement de données à caractère personnel de prendre les mesures techniques et organisationnelles nécessaires pour assurer la protection de telles données. On rappellera à ce propos l'arrêt de la Cour d'appel de Paris ayant prononcé la condamnation de la partie plaignante dans le cadre d'une affaire de *hacking* pour n'avoir pas suffisamment protégé les données à caractère personnel qu'elle traitait (Paris, 12e ch., 30 octobre 2002, *op. cit.*).

(201) Le dommage n'est sanctionné que lorsqu'il est la conséquence d'une introduction, une modification ou une suppression de données.

(202) En concours, le cas échéant, avec l'art. 550*ter*, §3, du C. pén.

IV. – *Questions particulières de droit pénal*

A. *Tentative*

58. Tentative de *hacking* punie comme le *hacking*. La tentative de *hacking* (interne ou externe) est incriminée au §4 de l'article 550*bis* du Code pénal et est punie des mêmes peines que le *hacking* lui-même (interne ou externe). Ceci est dérogatoire au régime habituel de la tentative, puisqu'en règle générale, la tentative d'un délit est punie moins sévèrement que l'infraction réalisée. Cette sévérité est justifiée, dans les travaux préparatoires, par la gravité intrinsèque du comportement (203). Cela va toutefois dans le sens de la réforme qu'avait proposée, en son temps, la Commission pour la révision du Code pénal de prévoir une peine identique pour la tentative et l'infraction consommée (204). On notera que la dérogation ne touche que la hauteur de la peine, la tentative de *hacking* restant soumise pour le surplus au régime des articles 51 et suivants du Code pénal. Il faudra donc, pour que la tentative de *hacking* soit établie, que la partie poursuivante apporte, sur le plan matériel, la preuve de ce que l'agent a mis en œuvre non seulement des actes préparatoires (par ailleurs incriminés – *cf. infra*), mais également des actes d'exécution (*cf. supra*, l'univocité circonstancielle). Dans ce cadre, les cas de tentative concerneront plus souvent des hypothèses d'accès illicite plutôt que de maintien.

À titre d'illustration, les travaux préparatoires citent l'essai automatisé de longues listes de mots de passe (205).

B. *Actes préparatoires*

59. Actes préparatoires comme infraction *sui generis*. Le §5 de la disposition incrimine particulièrement les actes préparatoires du *hacking* et érige en infraction spécifique la possession, la production, la vente, l'obtention en vue de son utilisation, l'importation, la diffusion ou la mise à disposition sous une autre forme d'un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour commettre un *hacking* (206).

(203) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 18.

(204) Commission pour la révision du Code pénal, *Rapport sur les principales orientations de la réforme*, Bruxelles, éd. du *Moniteur belge*, 1979, p. 86.

(205) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 20 0213/001, p. 18. Ce fut la technique utilisée dans l'affaire jugée à Eupen (Corr. Eupen, 15 décembre 2003, *op. cit.*).

(206) Cette disposition a été modifiée par la loi du 15 mai 2006, *M.B.*, 12 septembre 2006.

Il ne s'agit pas d'une circonstance aggravante du *hacking*, mais bien d'une infraction distincte (207), relevant de la catégorie des délits-obstacle (208). Il est donc possible que les actes préparatoires fassent l'objet de poursuites, indépendamment de tout *hacking*. Il s'agit d'un délit de mise en danger. Par cette disposition, le législateur a entendu sanctionner les personnes qui, mettant à disposition de tiers des logiciels ou d'autres outils permettant de violer la sécurité de systèmes informatiques, facilitent la commission de telles infractions et en encouragent la généralisation (209). Elle vise également l'escroquerie en matière de codes d'accès (210).

60. Actes préparatoires : élément matériel. Celui qui élabore, détient ou communique des *hackertools*, soit des logiciels ou des instructions destinés à faciliter le piratage, est passible d'une peine de prison allant de six mois à trois ans et/ou d'une amende comprise entre 26 et 100.000 EUR, peines devant être doublées en cas de récidive (211).

Alors que la formulation initiale de cette disposition limitait les *hackertools* aux seules données informatiques traitées, stockées ou transmises par un système informatique (tels des programmes, logiciels et codes d'accès permettant de faciliter le *hacking*), le texte remanié vise dorénavant tout dispositif principalement conçu ou adapté pour commettre un *hacking*, de sorte qu'un simple manuel ou une liste imprimée tombent dorénavant sous le coup de la disposition. Selon l'exposé des motifs de la loi du 15 mai 2006, il y a lieu d'entendre par dispositifs «les moyens d'accès ou autres outils qui sont conçus, par exemple, pour altérer voire détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques» (212).

On notera encore qu'alors que le texte initial sanctionnait la simple recherche (de sorte que la quête sur l'internet de logiciels facilitant le

(207) L'art. 5 de la décision-cadre de l'Union européenne relative aux attaques visant les systèmes d'information prévoit l'obligation pour les États membres de prendre les mesures nécessaires pour que soit rendu punissable le fait d'aider à commettre une atteinte à l'intégrité d'un système ou de données.

(208) «Dans ces infractions, la mise en danger, légalement présumée, ne demande plus à être établie dans le cas d'espèce. Le risque est la raison d'être de l'incrimination, il n'est plus un élément constitutif de l'infraction» (C. HENNAU et J. VERHAEGEN, *op. cit.*, p. 61).

(209) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 641. Les art. 51 et 53 du C. pén. incriminant la complicité n'auraient pu être opposés au fournisseur habituel de *hackertools* s'il n'avait pu être établi qu'il savait, au moment où il agissait, qu'il prêtait son concours à une infraction déterminée.

(210) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 18.

(211) C. pén., art. 550*bis*, §8. La récidive est ici aussi obligatoire, spécifique et temporaire.

(212) Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2003-2004, n° 51 1284/001, p. 6. Cette précision a été faite à la suite d'une demande du Conseil d'État en ce sens (Avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess. ord. 2003-2004, n° 50 1284/001, p. 15).

hacking était déjà punissable indépendamment de tout résultat), le texte modifié ne vise plus cette dernière situation (213).

À titre d'illustrations, relevons la publication de programmes ou d'instructions de *hacking*, la conception ou la mise à disposition de programmes soumettant des combinaisons de mots de passe, le trafic de mots de passe ou de numéros d'utilisation pour des logiciels, de codes secrets (214) ...

61. Actes préparatoires : élément moral. Avant d'être modifié par la loi du 15 mai 2006, l'article 550*bis*, §5, du Code pénal prévoyait que l'infraction n'était établie que pour autant que l'auteur ait été animé du dol spécial, à savoir une intention frauduleuse ou le dessein de nuire. Dorénavant, le texte prévoit qu'il faut, pour que la prévention soit établie, que l'auteur ait élaboré, détenu ou communiqué les *hackertools* «indûment».

Il nous apparaît que dans cette nouvelle version, la prévention se satisfait d'un dol général, le terme «indûment» exprimant, de façon certainement malhabile et malheureuse, une dimension volontaire. Cela exclut du champ d'application de la disposition la détention à des fins scientifiques ou professionnelles d'outils (logiciels ou autres) de sécurité informatique. À défaut de suivre cette interprétation, n'importe quelle société spécialisée en sécurité informatique risquerait une sanction pénale, ce qui ne correspondrait assurément pas à l'esprit ayant conduit à l'adoption de la règle et constituerait une entrave à la libre circulation d'informations générales en matière de techniques de protection informatique, liberté que le législateur a entendu protéger (215).

62. Dispositifs illicites d'accès à un service protégé. Parallèlement à cette disposition, il convient de rappeler qu'une autre loi interdit par ailleurs de fabriquer, d'importer, de distribuer, de vendre, de louer ou de détenir à des fins commerciales des dispositifs illicites, soit tout équipement ou logiciel conçu ou adapté pour permettre l'accès à un service protégé sous une forme intelligible sans l'autorisation du prestataire de services (216). Cette loi vise particulièrement les outils (les

(213) En tout état de cause, des poursuites du seul chef de recherche de *hackertools* auraient sans doute été peu fréquentes, étant donné qu'il aurait fallu prouver qu'en l'absence de toute possession de *hackertools*, l'auteur avait mis en œuvre des moyens d'exécution afin de s'en procurer.

(214) Le §5 vise également la recherche d'instruments de *hacking*. La loi ne précise pas s'il s'agit de la simple quête (sur l'internet ou par d'autres voies) de programmes facilitant le *hacking* ou de la recherche au sens scientifique (soit le développement) de tels programmes.

(215) *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 18.

(216) L. 12 mai 2003 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel relatifs aux services de la société de l'information (*M.B.*, 26 mai 2003, p. 28866). Cette loi transpose la directive européenne 98/84/CE sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel.

équipements matériels autant que les logiciels) permettant de casser des mesures techniques de sécurité en vue de bénéficier, de façon illicite, d'un service de la société de l'information normalement soumis à un accès conditionnel (tel un site permettant du téléchargement payant, p. ex.) (217). Cette incrimination spécifique, plus restrictive, entend ainsi protéger particulièrement, selon l'exposé des motifs, la juste rémunération des prestataires offrant l'accès à des bases de données, à des logiciels ou à des vidéos à la demande, notamment (218). Elle prévoit une peine de prison allant de huit jours à cinq ans ainsi qu'une amende comprise entre 25 et 25.000 EUR. En cas de récidive, les peines seront doublées pour autant que la nouvelle infraction ait été commise dans un délai de cinq ans à dater d'une condamnation coulée en force de chose jugée prononcée du chef d'une infraction aux dispositions de l'article 3 de ladite loi. La récidive sera donc spécifique et temporaire.

C. *Provocation à commettre un* hacking

63. Ordre ou incitation à commettre un *hacking*. La provocation (par la voie d'un ordre ou d'une incitation) à commettre un *hacking* est spécifiquement visée au §6 de l'article 550*bis* du Code pénal.

Il ne s'agit pas d'un cas de provocation au sens de l'article 66, alinéa 4, du Code pénal (qui prévoit que seront punis comme auteurs ceux qui auront provoqué directement à commettre un crime ou un délit), mais bien de l'incrimination particulière d'un comportement déterminé (219). La provocation à commettre un *hacking* fait en effet l'objet d'une définition particulière et donne lieu à une sanction plus lourde que le *hacking* lui-même.

La provocation doit consister en un ordre ou une incitation à *hacker*. Ces notions d'ordre et d'incitation ne sont pas précisées, ni dans la loi ni dans les travaux préparatoires. Il convient dès lors de les entendre dans le sens courant que leur prête le langage usuel. Il nous apparaît que la notion d'ordre implique, sinon un lien de hiérarchie ou de subordination, à tout le moins un rapport interpersonnel unissant le donneur

(217) Ainsi qu'il est précisé à l'art. 1er de la loi, on entend par service de la société de l'information tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de service. Une liste figurant en annexe de la loi reprend différents types de services ne tombant pas sous le coup de la loi car une de ces conditions vient à manquer. Ainsi en est-il, p. ex., des services de distribution automatique de billets de banque ou des services de marketing direct par téléphone.

(218) *Doc. parl.*, Ch. repr., sess. ord. 2002-2003, n° 51 2153/001, p. 4.

(219) La provocation consistant à encourager de façon générale le *hacking* par la mise à disposition d'outils ou d'instructions n'est pas visée par le §6, mais par le §5.

d'ordre à la personne appelée à *hacker* de nature à faire naître dans le chef de cette dernière un sentiment d'obligation de répondre positivement à l'injonction qui lui a été donnée. Quant à la notion d'incitation, il nous semble qu'elle doit être entendue comme relative à un encouragement à commettre l'infraction. Elle se rapproche en cela, dans son esprit, de la disposition reprise à l'article 1er de la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, qui sanctionne également une incitation (220). On relèvera encore que la loi n'exige pas que l'ordre ait été assorti d'une menace ou que l'incitation ait été accompagnée d'une offre de récompense (221). On relèvera également que la loi n'a prévu ni cause d'excuse, ni exception à l'incrimination en faveur du *hacker* ayant agi sur ordre (222).

La loi ne précise pas si la provocation doit avoir été suivie d'effets (223). Le droit pénal étant d'interprétation stricte, il ne pourrait être question de rajouter une condition d'existence à l'infraction. En ces circonstances, il nous apparaît que la prévention de provocation à commettre un *hacking* peut être suffisamment établie en dehors même de toute réalisation effective d'accès ou de maintien non autorisé dans un système informatique par la personne à qui l'ordre a été donné ou que l'auteur entendait inciter (224), pour autant toutefois qu'il soit établi que la provocation était directe, c'est-à-dire en lien et pouvoir causal direct avec un *hacking* déterminé. Le seul encouragement général à *hacker* ne relève pas de cette disposition mais, le cas échéant, du §5 de l'article 550*bis* (*cf. supra*).

La loi ne prévoit pas de dol spécial. Il y a donc lieu de considérer, dans le silence du texte, que l'article 550*bis*, §6, se satisfait d'un dol général dans le chef du commanditaire. Ce qui n'empêche en rien que l'auteur du *hacking* lui-même soit, lui, animé d'un dol spécial (225).

À titre d'illustrations, citons le cas de l'employé qui convainc un collègue plus doué que lui en informatique d'aller consulter la mémoire de l'agenda électronique de son patron.

(220) Voy. égal. l'art. 434 du C. pén., qui sanctionne ceux qui auront fait arrêter ou fait détenir de façon arbitraire, ainsi que l'art. 380*bis*, qui prévoit la provocation à la débauche.

(221) Même si, en ce dernier cas, l'existence d'une telle récompense ou menace contribuera assurément à prouver la matérialité de l'infraction.

(222) Par comparaison avec les art. 152 et 260 du C. pén.

(223) Contrairement à la provocation comme acte de participation, qui suppose que l'infraction ait été réalisée ou ait, à tout le moins, fait l'objet d'une tentative punissable.

(224) Dans le même sens, C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 643

(225) Lors d'un *hacking* interne ou lors d'un *hacking* externe avec la circonstance aggravante qu'il a été commis avec intention frauduleuse.

En cas de provocation, le commanditaire ou l'instigateur est puni plus sévèrement que le *hacker* lui-même, puisqu'il risque une peine d'emprisonnement de six mois à cinq ans et/ou une amende allant de 100 à 200.000 EUR, soit une des amendes les plus lourdes du Code pénal (226), laquelle peut encore être doublée en cas de récidive (227). La raison d'être de cette sévérité réside dans le fait que, selon le législateur, si auparavant le *hacking* consistait, dans bien des cas, en un divertissement pour des jeunes fanatiques d'informatique, il serait devenu une activité de criminels professionnels engageant de telles personnes pour accomplir leurs desseins (228).

Le cas échéant, une peine de travail pourra être préférée (229).

S'agissant d'une infraction instantanée, la prescription prendra cours dès que l'ordre ou l'incitation à *hacker* auront été pleinement formulés à destination de la personne appelée à commettre le *hacking*. Cette infraction étant distincte de l'infraction de *hacking*, il se peut que le point de départ de la prescription diffère pour l'une et l'autre de ces infractions.

D. *Recel de données informatiques obtenues à la suite d'un* hacking

64. Recel de données obtenues à la suite d'un *hacking*. Le §7 de l'article 550*bis* du Code pénal sanctionne d'une peine de prison allant de six mois à trois ans et/ou d'une amende allant de 26 à 100.000 EUR quiconque détient, révèle à une autre personne, divulgue ou fait un usage quelconque de données obtenues à la suite d'un *hacking*. Ces peines seront doublées en cas de récidive (230).

Cette disposition a été insérée afin d'incriminer le recel de biens immatériels. De tels biens étaient exclus de la définition de l'article 505 du Code pénal (et des articles suivants), qui visait notamment la détention de *choses* à l'origine illicite (231). Or, sauf à figurer sur un support matériel

(226) À titre de comparaison, l'art. 324*ter*, §4, du C. pén., relatif au dirigeant d'une organisation criminelle, prévoit une amende comprise entre 1.000 et 200.000 EUR. Seul l'art. 490*bis* du C. pén. relatif à l'organisation frauduleuse d'insolvabilité prévoit une amende plus lourde (500.000 EUR).

(227) C. pén., art. 550*bis*, §8. la récidive est obligatoire, spécifique et temporaire.

(228) *Doc. parl.*, Ch. repr., sess. ord. 2002-2003, n° 51 2153/001, p. 18.

(229) C. pén., art. 37*ter*, §1er, al. 2.

(230) C. pén., art. 550*bis*, §8. La récidive est ici aussi obligatoire, spécifique et temporaire.

(231) Sur la controverse relative à l'applicabilité de l'art. 505 du C. pén. aux données informatiques, voy. O. VANDEMEULEBROEKE, «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)», *op. cit.*, p. 209. Voy. égal. la décision rendue par le Tribunal correctionnel de Bruxelles le 24 juin 1993 assimilant les programmes informatiques à des «choses» (Corr. Bruxelles, 24 juin 1993, *J.L.M.B.*, 1994, p. 444; *J.T.*, 1995, p. 685; Corr. Malines, 16 février 2006, *Nullum Crimen*, 2007, p. 161).

(disque dur, CD-Rom, disquette, clé USB ...) susceptible d'être recelé, les données elles-mêmes ne pouvaient être assimilées à de telles choses (232).

Le recel de données informatiques issues d'un *hacking* est une infraction *sui generis*, et non une circonstance aggravante du *hacking*. Elle peut dès lors être poursuivie indépendamment du *hacking* et donner lieu à une condamnation alors même, par exemple, que le *hacker* serait demeuré inconnu. À ce propos, on relèvera qu'alors que le recel de droit commun n'exige pas qu'il soit précisé, dans la décision de condamnation, quel crime ou délit avait été à la base du recel (233), il nous apparaît, en ce qui concerne le recel de données informatiques issues d'un *hacking*, qu'il sera nécessaire, compte tenu de la formulation même de la disposition, que le juge précise, si pas qui fut l'auteur du *hacking* ayant conduit au recel, à tout le moins que les données recelées ont été obtenues à la suite d'un *hacking* commis par un tiers. Il ne peut en effet être question de recel de données informatiques si celui qui les détient les a obtenues par suite d'un *hacking* qu'il a lui-même commis, puisqu'il s'agit en ce cas d'une circonstance aggravante du *hacking* (234). Un bémol toutefois : l'usage quelconque fait des données obtenues à la suite d'un *hacking* ne relève pas de la circonstance aggravante du *hacking* telle que prévue au §3, 2°, de l'article 550*bis* du Code pénal, mais constitue bel et bien un fait de recel informatique, puisque la circonstance aggravante ne vise que l'usage du système informatique visité, et non celui des données qu'il stocke, traite ou transmet.

La formulation générale de la disposition est analogue à celle relative à la divulgation du contenu de communications ou télécommunications privées écoutées ou enregistrées illégalement (235). On relèvera toutefois que la disposition ne vise que les données issues d'un *hacking* et ne recouvre donc pas la détention de données obtenues à la suite du vol de leur support (236) (sauf à considérer ledit support comme un système informatique, comme une carte à puce p. ex.). En cela, la prévention de recel de données informatiques, infraction de conséquence (237), ne connaît qu'une portée limitée, inférieure à celle existante en droit luxembourgeois notamment (238).

(232) Pour une décision allant en sens contraire, voy. Corr. Bruxelles, 24 juin 1993, *J.T.*, 1995, p. 685 : «Un logiciel ou programme informatique, indépendamment même de son support – ou disquette – ne constitue pas un bien immatériel, possède une valeur économique propre et est susceptible d'un transfert de possession qui peut être constaté matériellement».

(233) Cass., 18 décembre 1991, *Pas.*, 1992, I, p. 209; Cass., 9 juin 1999, *Pas.*, 1999, p. 340. En tous cas en l'absence de conclusions sur ce point (Cass., 26 mars 1991, *Pas.*, 1991, I, p. 402).

(234) Reprise des données – C. pén., art. 550*bis*, §3, 1°.

(235) C. pén., art. 314*bis*, §2.

(236) En ce cas, c'est le support lui-même qui est recelé (C. pén., art. 505).

(237) A. Masset et C. Pevée, «À la recherche de la notion de délit financier», in *Les délits financiers/De financiele misdrijven*, Bruxelles, Bruylant, 2001, pp. 21-22.

65. Recel de données informatiques sur le plan matériel. Au niveau de l'élément matériel, l'infraction de recel de données informatiques suppose que l'auteur ait détenu, révélé à une autre personne, divulgué ou fait un usage quelconque de données issues d'un *hacking*. La notion de *détention* des données n'est pas définie. Couvre-t-elle le seul stockage dans le système informatique de l'utilisateur des données recelées? Sur le plan strictement matériel, il nous semble que cela puisse suffire (239). Sur le plan moral toutefois, cela suppose qu'il soit établi que la mémorisation des données avait été faite volontairement (*cf. infra*) (240). La notion d'usage quelconque n'a pas été définie non plus. Elle tend à donner au texte une portée large, puisque l'auteur pourra être sanctionné quel que soit l'usage qu'il aura fait des données recueillies.

66. Recel de données informatiques sur le plan moral. Au niveau de l'élément moral, la disposition prévoit qu'il faut que l'auteur ait su que les données recelées avaient été obtenues à la suite d'un *hacking* externe ou interne, soit qu'il ait été animé d'un dol spécial implicite (241). Cette connaissance doit exister au moment du recel, c'est-à-dire au plus tard au moment où les données ont été reçues (242). Il n'est toutefois pas

(238) Le législateur luxembourgeois a préféré modifier la définition de l'art. 505 du C. pén. luxembourgeois pour y insérer les termes «biens incorporels». Voy. à ce propos, M. Durin, O. Leroux, A. Misonne, C. Poullet et R. Vuitton, *Le commerce électronique en droit luxembourgeois – Commentaire de la loi (modifiée) du 14 août 2000 relative au commerce électronique* (A. Prüm, Y. Poullet et E. Montero dir.), Bruxelles, Larcier, 2005, pp. 363 et s.

(239) L'acte matériel de recel est en effet la détention d'un objet, au sens de le garder en sa possession ou de le posséder juridiquement, sans que cette possession ne soit matérialisée (Cass., 5 octobre 1999, *Pas.*, 1999, p. 1265). La jurisprudence la plus ancienne de la Cour de cassation utilise d'ailleurs le terme «recevoir». Ce qui est donc visé est plus exactement l'entrée en possession ou en détention de la chose (Cass., 1er août 1880, *Pas.*, 1880, I, p. 284; Cass., 30 janvier 1911, *Pas.*, 1911, I, p. 114).

(240) La Cour de cassation de France a eu l'occasion d'approcher cette question, dans un contexte tout à fait différent, il est vrai. En l'occurrence, il lui était revenu de déterminer si l'art. 227-23 du C. pén. français, qui incrimine notamment le fait de détenir une image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique, recouvrait l'hypothèse de telles images stockées dans les fichiers temporaires de l'utilisateur. En d'autres termes, cela suffisait-il pour caractériser la détention au sens de l'art. 227-23? Pour la Cour de cassation de France, la réponse était non, les images n'ayant été ni imprimées ni enregistrées sur un support autre que la mémoire cache (Cass. fr., 5 janvier 2005, *www.juritel.com*). Il nous semble toutefois que la condition de la détention sera remplie lorsqu'il sera établi que les données auront été stockées volontairement et de façon structurée dans la mémoire cache.

(241) Voy. à ce propos, en ce qui concerne le recel de droit commun : Cass., 4 juin 1996, *Pas.*, 1996, I, p. 208; *J.T.*, 1997, p. 182; Cass., 4 mars 1997, *Pas.*, 1997, I, p. 118; Cass., 12 janvier 2000, *Pas.*, 2000, p. 22.

(242) Le recel de droit commun suppose la connaissance préexistante ou concomitante à la prise de possession de l'objet de son origine illicite (voy. not. Cass., 25 février 1929, *Pas.*, 1929, I, p. 102;

nécessaire que les données aient été commandées par le receleur au *hacker* (243). Il n'est pas nécessaire non plus que le receleur ait eu connaissance des éventuelles circonstances aggravantes du *hacking*.

Selon une certaine jurisprudence de la Cour de cassation, en matière de recel de droit commun, il faut également, pour que la prévention soit établie, que l'auteur ait été animé de l'intention frauduleuse de conserver la chose recelée (244) et qu'il ait eu la volonté de la soustraire aux recherches du légitime titulaire ou de la justice, c'est-à-dire la volonté de ne pas la restituer (245). Une partie de la doctrine, s'appuyant sur d'autres arrêts de la Cour, considère que ces éléments ne sont pas requis, ni explicitement, ni implicitement, par le texte de l'article 505 du Code pénal (246).

La connaissance de l'origine illicite des données peut être déduite de la nature des données ou de toute autre circonstance factuelle de nature à éveiller la méfiance de celui qui en prend possession (247). Le juge peut également déduire cet élément de connaissance des comportements ultérieurs du receleur (248), et en particulier de sa volonté de les dissimuler (ainsi en ira-t-il, p. ex., des données cachées dans des fichiers dont l'extension aura été modifiée, de celles dont les supports auront été dissimulés, des données stockées de façon volontairement structurée dans des fichiers temporaires ...).

67. Recel de données informatiques : infraction instantanée. Le recel de droit commun étant considéré comme un délit instantané (249),

Cass., 9 juin 1936, *Pas.*, 1936, I, p. 286; Cass., 27 juin 1949, *Pas.*, 1949, I, p. 475; Cass., 21 décembre 1976, *Pas.*, 1976, I, p. 448; Cass., 20 mai 1981, *Pas.*, 1981, I, p. 1094; Cass., 18 décembre 1991, *Pas.*, 1991, I, p. 402; *Arr. cass.*, 1991, p. 355; *Rev. dr. pén.*, 1992, p. 433; *J.L.M.B.*, 1993, p. 681). Si le juge constate que le prévenu a pris connaissance de l'origine illicite des données après la prise de détention, il doit prononcer l'acquittement, quand bien même il estimerait cette attitude moralement blâmable (pour une décision rendue en matière de recel de droit commun : Corr. Gand, 15 septembre 1997, *T.G.R.*, 1998, p. 34).

(243) En ce cas, il y aurait lieu d'appliquer l'art. 550*bis*, §6, relatif au commanditaire du *hacking* (C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 645).

(244) La durée de conservation est sans importance, de même que l'éventuelle suppression de celles-ci par le receleur (par analogie avec le recel de droit commun – Cass., 24 mars 1958, *Pas.*, 1958, I, p. 823).

(245) Par analogie avec le recel de droit commun. Cass., 15 mai 1950, *Pas.*, 1950, I, p. 649; Cass., 14 octobre 1957, *Pas.*, 1958, I, p. 127; Cass., 24 mars 1958, *Pas.*, 1958, I, p. 823; Cass., 24 mai 1967, *Pas.*, 1967, I, p. 1130; Cass., 21 décembre 1976, *Pas.*, 1977, I, p. 448; *Arr. cass.*, 1977, I, p. 447.

(246) J. SPREUTELS, «L'élément moral du recel», obs. sous Cass., 2 mai 1977, *J.T.*, 1978, p. 29. Cass., 3 novembre 1975, *Pas.*, 1976, I, p. 283; *Rev. dr. pén.*, 1975-1976, p. 1005, obs. Ch.-H. HENRION; Cass., 25 septembre 1973, *Pas.*, 1974, I, p. 78; Cass., 31 janvier 1984, *Pas.*, 1984, I, p. 608.

(247) Par analogie avec le recel de droit commun : Cass., 9 juin 1999, *Pas.*, 1999, p. 504.

(248) Cass., 4 mars 1997, *Pas.*, 1997, I, p. 118.

(249) Not., Anvers, 1er avril 1993, *R.W.*, 1993-1994, p. 130; Cass., 11 mai 2004, *Pas.*, 2004, p. 794. On relèvera que différentes initiatives parlementaires ont été déposées ces dernières années en vue de faire du recel un délit continu.

il en ira de même du recel de données informatiques obtenues à la suite d'un *hacking*, de sorte que le point de départ de la prescription sera la réception des données recelées, puisque l'infraction sera entièrement consommée dès ce moment-là (250). Cette circonstance n'empêche toutefois pas que de mêmes données obtenues à la suite d'un *hacking* puissent faire l'objet de différentes infractions de recel de données informatiques commises successivement par d'autres auteurs ou complices (251).

On relèvera encore, par analogie avec le recel de droit commun, que la répression du recel de données informatiques ne nécessitera pas que l'auteur du *hacking* ait été identifié ni le responsable du système informatique visité.

68. Recel de données informatiques : observations quant aux peines. Ainsi que précisé ci-avant, le recel de données informatiques est puni d'un emprisonnement de six mois à trois ans et/ou d'une amende comprise entre 26 et 100.000 EUR. La peine privative de liberté est inférieure à celle prévue par le Code pour le recel de droit commun, qui peut être puni d'un emprisonnement de quinze jours à cinq ans. Elle est également unique, en ce sens qu'elle n'est pas susceptible d'augmenter en raison de la gravité du *hacking* au moyen duquel les données ont été obtenues, contrairement à la peine de prison du recel consécutif à un crime (252).

La peine d'amende est identique.

La loi n'a pas prévu la possibilité pour le juge de prononcer une interdiction conformément à l'article 33 du Code pénal (253) ni sur la base de l'arrêté royal relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines professions ou activités (254), alors que le recel ou toute autre opération relative à des choses tirées d'une infraction y est visé.

E. *Récidive*

69. Récidive temporaire, spéciale et obligatoire. La récidive est visée au §8 et appelle les mêmes commentaires que les récidives de faux informatique et de fraude informatique, à savoir qu'elle n'existe

(250) Le recel de données informatiques étant une infraction distincte du *hacking*, sa prescription sera distincte de celle du *hacking* à la suite duquel les données ont été obtenues.

(251) Par analogie avec le recel de droit commun (Cass., 4 mars 1997, *Pas.*, 1997, I, p. 118).

(252) L'art. 506 du C. pén. prévoit une augmentation de la peine du receleur en fonction de la gravité du crime ayant conduit au recel.

(253) Alors que cette interdiction est visée à l'art. 505, al. 5, du C. pén.

(254) A.R. n° 22 du 24 octobre 1934 (*M.B.*, 27 octobre 1934).

qu'en cas de nouvelle infraction commise dans les 5 ans du prononcé. Elle est également spéciale et obligatoire (255).

Depuis l'entrée en vigueur de la loi, très peu de décisions ont été publiées. On notera toutefois cette décision du Tribunal correctionnel d'Eupen, qui fut la première (256).

V. – *Questions particulières de procédure*

70. Écoutes de télécommunications privées. L'article 550*bis* du Code pénal est repris dans la liste de l'article 90*ter* du Code d'instruction criminelle relatif aux écoutes, prises de connaissance et enregistrement de communications et de télécommunications privées (257). Des écoutes sont donc possibles. On notera à ce propos que les écoutes dont il est question peuvent porter sur des télécommunications électroniques. Outre ces écoutes (relatives au contenu de la communication), des mesures d'identification et de repérage peuvent bien entendu être ordonnées.

§ 4. – Sabotage informatique et infractions voisines (C. pén., art. 550*ter*)

71. Notion. Le sabotage informatique a été introduit dans le Code pénal, à l'article 550*ter*, par l'article 6 de la loi du 28 novembre 2000 relative à la criminalité informatique. Par l'adoption de cette disposition, le législateur a entendu répondre aux insuffisances du droit pénal traditionnel, qui ne prenait en compte que les destructions et dommages se rapportant à des objets corporels (258).

En substance, le sabotage informatique vise l'atteinte à l'intégrité d'un système informatique ou des données qu'il contient, stocke ou transmet.

(255) Il est renvoyé aux développements consacrés à ces notions dans l'étude du faux informatique.

(256) Cas d'application de l'art. 550*bis*, §1er, du C. pén. : Corr. Eupen, 15 décembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 61 et s., note O. Leroux ; *Computerr.*, 2001, pp. 129-130. En l'espèce, il était reproché au prévenu d'avoir tenté de s'introduire à trois reprises au moins au moyen d'un programme de piratage dans une base de données stockée sur un système informatique appartenant à un concurrent et ce, à partir de son ordinateur personnel et via une simple connexion Internet. Identifié par son adresse IP reprise dans les *log-books* de la machine visée, le prévenu avait reconnu les faits. Il avait bénéficié d'une suspension du prononcé et avait été condamné à payer la somme provisionnelle de 1.000 EUR à titre de dommages et intérêts. Corr. Hasselt, 21 janvier 2004, *Computerr.*, 2004, p. 130 et s. ; Corr. Bruxelles, 6 janvier 2004 (inédit, cité par E. Roger France, «La criminalité informatique», *op. cit.*, p. 118).

(257) C. instr. crim., art. 90*ter*, §2, 13°*bis*.

(258) Sous réserves de dispositions particulières, telle la loi du 30 juin 1994 relative aux programmes d'ordinateurs, qui punit la modification des programmes sans le consentement du titulaire des droits (art. 5 et 10), et malgré certaines applications parfois peu satisfaisantes des art. 521, 523, 527 et 529 du C. pén. Voy. à ce propos, O. Vandemeulebroeke, «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)», *op. cit.*, p. 202.

La disposition ne vise pas la destruction ou le dommage causé au support des données, qui relève du droit commun (et des dispositions relatives aux destructions et dégradations de biens mobiliers – C. pén., art. 510 et s.) (259).

I. – *Éléments constitutifs*

72. Le sabotage informatique sur le plan matériel. Les éléments constitutifs du sabotage informatique sont, sur le plan matériel, une introduction, une modification ou un effacement de données ou une modification de l'utilisation normale des données qui n'ont pas été autorisés par le responsable du système informatique concerné. La destruction d'une carte magnétique donnant accès à un système informatique protégé n'est donc pas un sabotage informatique, mais une destruction au sens des articles 510 et suivants du Code pénal (260). De même, la destruction d'un ordinateur ou d'un GSM n'est pas un sabotage informatique.

Les opérations de sabotage informatique peuvent avoir été faites directement ou indirectement, sans que la loi ne précise la portée de ces adverbes (sans doute vise-t-on les sabotages commis à distance – par relais).

Compte tenu de la formulation générale utilisée, il semble que toute modification de données stockées, traitées ou transmises par un système informatique soit susceptible, dès lors qu'elle n'a pas été autorisée, d'être constitutive d'un sabotage. Il peut s'agir de l'introduction d'un virus, d'une bombe logique ou d'un cheval de Troie, mais aussi, plus simplement, de la modification du mot de passe d'un utilisateur, de la suppression d'un fichier ou de la création d'un nouveau (261) ... La loi ne prévoit en effet pas, contrairement à l'idée que l'intitulé de l'infraction pourrait suggérer, que ces opérations aient causé un dommage. Le dommage n'est pas un élément constitutif de l'infraction, mais seulement une circonstance aggravante (*cf. infra*). L'introduction de données informatiques dans un système destinées à l'endommager est donc punissable comme sabotage informatique, même si ces données ont été

(259) Par un arrêt du 10 novembre 2004, la Cour de cassation a eu l'occasion de préciser que les dommages occasionnés à des données ou programmes informatiques relevaient de l'art. 550*ter* du C. pén., et non de l'art. 523 du même Code (Cass., 10 novembre 2004, R.G. n° P.04.0974.F, *www.cass.be*).

(260) C. Meunier, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 648.

(261) Pour d'autres hypothèses, voy. F.-J. Pansier et E. Jez, *La criminalité sur l'internet*, coll. Que sais-je?, Paris, P.U.F., 2000, p. 107.

neutralisées ou si, pour une raison quelconque, elles n'ont pu produire leur effet (262).

On relèvera par ailleurs qu'une autre disposition (*cf. infra*) incrimine particulièrement le fait d'occasionner un dommage, quel qu'il soit, par l'utilisation d'un réseau ou d'un service de communications électroniques ou d'autres moyens de communications électroniques (263). En cette hypothèse, la loi ne distingue pas selon que le dommage a été causé à des données ou à un système informatique.

73. Le sabotage informatique sur le plan moral. Sur le plan moral, le sabotage informatique se satisfait d'un simple dol général. Il faut donc, mais il suffit, que l'auteur de l'infraction ait eu conscience de ce qu'il exécutait une opération illicite (264). De cette façon, échappe à la répression, celui qui transmet, à son insu, un virus informatique (265) ou celui qui installe sur un disque dur un logiciel vicié perturbant le fonctionnement de la machine.

Dans sa première mouture, le texte de la loi exigeait que l'auteur ait été animé du dol spécial, à savoir le dessein de nuire. Cela a été modifié par la loi du 15 mai 2006, qui a ramené l'élément moral au simple dol général en vue d'accorder la loi belge aux dispositions de la Convention (266). La preuve de ce dol devra bien entendu être apportée par la partie poursuivante.

Toutefois, si le dol spécial n'est plus un élément constitutif de l'infraction, il constitue dorénavant une circonstance aggravante, puisque si l'auteur a agi avec une intention frauduleuse ou dans le but de nuire, il risquera une peine comprise entre six mois et cinq ans de prison (*cf. infra*).

II. – *Circonstances aggravantes*

La loi a prévu une circonstance aggravante subjective (§ 1er, al. 2) et deux circonstances aggravantes objectives (§§ 2 et 3).

(262) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 647.

(263) Art. 145, § 3, 2°, de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.

(264) Cette conscience doit être doublée de la volonté ou de l'acceptation de commettre l'infraction.

(265) S. EVRARD, «La loi du 28 novembre 2000 relative à la criminalité informatique», *op. cit.*, p. 244.

(266) L. 15 mai 2006 modifiant les articles 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal, *M.B.*, 12 septembre 2006.

74. L'intention frauduleuse ou le but de nuire. S'il est établi que l'auteur a agi avec intention frauduleuse ou dans le but de nuire, la peine sera portée à six mois à trois ans d'emprisonnement et/ou une amende comprise entre 26 et 25.000 EUR (267).

75. Dommage aux données. La première circonstance aggravante objective est relative au dommage causé aux données stockées, transmises ou traitées par le système informatique concerné ou tout autre système informatique. Elle vise l'altération faite aux données elles-mêmes par opposition au dommage causé au système qui les stocke, traite ou transmet. Lorsque la circonstance aggravante sera rencontrée, les peines seront de six mois à cinq ans d'emprisonnement et/ou une amende comprise entre 26 et 75.000 EUR, doublées en cas de récidive (268).

76. Dommage au système. La seconde circonstance aggravante objective est relative au dommage causé au système informatique lui-même ou à tout autre système informatique. Le législateur vise ici notamment le blocage total ou partiel du système informatique visé par le sabotage, par exemple à la suite d'une introduction d'un grand nombre de requêtes ayant eu pour effet de surcharger le serveur et d'entraîner son blocage ou d'altérer son bon fonctionnement. Relève également de cette circonstance aggravante, le dommage physique occasionné au système à la suite d'une introduction, une modification ou une suppression de données. Certains virus, en effet, peuvent entraîner le bris d'un disque dur, donnant ainsi corps à une criminalité à l'origine dématérialisée. Lorsqu'un tel dommage aura été causé, la peine sera d'autant plus élevée, puisqu'elle sera comprise entre un an et cinq ans d'emprisonnement et/ou une amende comprise entre 26 et 100.000 EUR, ces peines devant être doublées en cas de récidive (269). On relèvera que lorsque le dommage aura été physiquement occasionné au système à la suite d'un sabotage informatique, la peine encourue par le saboteur est plus importante que celles prévues par les articles 523, 528 et 533 du Code pénal.

Ainsi que le souligne C. Meunier, l'atteinte aux données entraînant le plus souvent des répercussions sur le fonctionnement du système

(267) C. pén., art. 550*ter*, § 1er, al. 2, tel que mod. par L. 15 mai 2006, entrée en vigueur le 22 septembre 2006.

(268) C. pén., art. 550*ter*, § 5.

(269) Le législateur justifie cette répression accrue dans les termes suivants : «compte tenu de l'importance que prennent les systèmes informatiques dans notre société, le fait d'empêcher le bon fonctionnement d'un système informatique est puni plus sévèrement que le simple fait de causer un dommage aux données» (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 19).

informatique, il est probable que les deux circonstances aggravantes trouveront à s'appliquer conjointement et que, ces deux avaries étant difficiles à distinguer l'une de l'autre, la seconde sera plus souvent retenue (270).

Enfin, lorsque le dommage occasionné aux données ou au système aura été la conséquence involontaire d'un *hacking*, il constituera une circonstance aggravante du *hacking* (*cf. supra*). Dans ce cas, la peine pourra être majorée et ce, même si le dommage n'a pas été causé par une introduction, une modification ou une suppression de données.

III. – *Questions particulières de droit pénal*

A. *La facilitation du sabotage informatique*

77. Les dispositifs de sabotage. Le §4 de l'article 550*ter* du Code pénal introduit dans l'arsenal répressif une infraction spécifique relative à la facilitation du sabotage (271).

Cette infraction est indépendante du sabotage lui-même et peut donc faire l'objet de poursuites alors même qu'aucun sabotage n'aurait été commis. Il s'agit d'un délit formel ou délit de mise en danger incriminant l'attitude consistant à favoriser l'exécution de l'infraction par un tiers (272). L'économie de cette disposition est à rapprocher de l'article 550*bis*, §5, relatif aux *hackertools* (*cf. supra*).

Cette disposition vise très certainement la publication d'informations aidant le sabotage informatique ou la création de virus informatiques.

78. La facilitation du sabotage informatique sur le plan matériel. La disposition sanctionne d'une peine d'emprisonnement comprise entre six mois et trois ans et/ou d'une amende comprise entre 26 et 100.000 EUR la possession, la production, la vente, l'obtention en vue de son utilisation, l'importation, la diffusion ou la mise à disposition sous une autre forme d'un dispositif, y compris des données informatiques, principalement conçu ou adapté pour commettre un sabotage informatique.

(270) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 648-649.

(271) Cette disposition a été modifiée par la loi du 15 mai 2006.

(272) Voy. l'art. 335 du C. pén., qui sanctionne ceux qui auront facilité l'évasion d'un détenu, ainsi que l'art. 3, §2, de la loi du 24 février 1921, qui vise spécifiquement celui qui aura facilité à autrui l'usage de substances stupéfiantes.

La notion de «dispositif» est identique à celle utilisée dans la définition de l'article 550*bis*, §5, du Code pénal, relatif aux *hackertools*. Il est donc renvoyé à l'étude de cette disposition.

79. La facilitation du sabotage informatique sur le plan moral. L'élément moral de cette infraction particulière est le dol général. Le texte prévoit qu'il faut que l'auteur ait agi «indûment». Dans sa première mouture, l'article 550*ter*, §4, prévoyait le dol spécial (l'intention frauduleuse ou le but de nuire) et précisait qu'il fallait que l'auteur ait eu la connaissance que les données pouvaient être utilisées pour causer un dommage à des données ou pour empêcher totalement ou partiellement le fonctionnement correct d'un système informatique. Bien que la version modifiée par la loi du 15 mai 2006 ne fasse plus référence à cette connaissance, il nous apparaît que cette condition demeure implicitement de mise, le dol général emportant cet élément intentionnel.

Il en résulte que la possession involontaire et ignorée de dispositifs de sabotage ne tombe pas sous le coup de la disposition. De même, la possession justifiée par un usage licite (scientifique ou professionnel) de tels dispositifs échappe également à la répression. Les termes «principalement conçu ou adapté pour permettre la commission des infractions» ainsi que «alors qu'il sait que ces données peuvent être utilisées pour causer un dommage» étayent cette thèse.

B. *Récidive*

80. Récidive spéciale, temporaire et obligatoire. La récidive est prévue au §5. Elle prévoit que les peines seront doublées en cas de nouvelle infraction commise dans les cinq ans du prononcé d'une condamnation pour des faits de criminalité informatique (273). Cette augmentation concerne les peines de l'infraction elle-même comme celles de la tentative et des circonstances aggravantes.

C. *Tentative de sabotage informatique*

81. Tentative punie comme le sabotage. La tentative de sabotage informatique est incriminée au §6 de l'article 550*ter* du Code pénal et est punie des mêmes peines que le sabotage lui-même. À l'origine, elle n'était pas incriminée par la loi criminalité informatique, alors qu'elle

(273) À savoir une condamnation pour des faits visés aux art. 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis* du C. pén. *Cf. supra*, les développements consacrés à la question de la récidive dans le cadre de l'étude du faux informatique.

l'était tant par la Convention cybercriminalité du Conseil de l'Europe que par la décision-cadre de l'Union européenne. C'est en vue de mettre la disposition belge en conformité avec ces textes supranationaux que le législateur a, par la loi du 15 mai 2006, inséré ce §6 à l'article 550*ter* du Code pénal.

82. Écoutes de télécommunications privées. Tout comme le faux informatique, la fraude informatique et le *hacking*, le sabotage informatique est susceptible de donner lieu à des écoutes ainsi qu'à des mesures de repérage et d'identification.

§ 5. – Refus d'information et de collaboration (C. instr. crim., art. 88*quater* et 90*quater*, §4)

83. Notion. Dans le cadre d'une recherche informatique effectuée conformément à l'article 88*quater* du Code d'instruction criminelle ou dans le cadre d'une écoute d'une communication ou télécommunication privée, il est possible que les enquêteurs se trouvent confrontés à de grandes difficultés, voire à l'impossibilité, d'accéder au système informatique, de décrypter des données ou d'ouvrir des fichiers en raison soit de la complexité des réseaux ou du système, soit de la faiblesse de leurs moyens. C'est pour surmonter ces difficultés que la loi a prévu la possibilité, pour les autorités chargées des poursuites, de requérir (274) les services de toute personne ayant une connaissance particulière du système.

84. Le refus de collaboration dans le cadre de la recherche informatique. L'article 88*quater* du Code d'instruction criminelle relatif à la recherche informatique permet au juge d'instruction d'ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique soumis à la recherche ou des méthodes de cryptage utilisées de fournir des informations sur ce système ou sur les méthodes de cryptage. Sur cette même base, il peut également ordonner à toute personne appropriée de mettre elle-même le système informatique en marche ou, selon le cas, de rechercher, rendre accessible ou inaccessible, copier ou retirer des données pertinentes (275).

(274) La collaboration contrainte dont il est question ne constitue ni un témoignage ni une expertise, mais bien une réquisition comparable à celles prévues à l'art. 42, al. 1er, de la loi du 4 juillet 1992 sur la fonction de police ou aux art. 88*bis* et 90*ter* du C. instr. crim. On notera par ailleurs que la loi n'a prévu ni rémunération ni indemnisation pour les personnes requises.

(275) C. instr. crim., art. 88*quater*, §2.

La collaboration peut donc être exigée pour donner des informations sur le système informatique ou pour intervenir sur celui-ci.

La demande d'informations pourra porter sur des informations verbales quant au fonctionnement du système informatique lui-même ou d'un programme particulier, mais il pourra s'agir également de la demande de remise d'un mot de passe, d'une clé de cryptage, du schéma du système informatique ou du réseau, de la description des mesures de sécurité protégeant le système informatique et des outils nécessaires pour les neutraliser.

Les personnes visées par cet article ne sont pas particulièrement définies. Les personnes susceptibles d'être concernées par ces obligations sont donc nombreuses. On pense notamment à l'informaticien en charge du système informatique concerné par la mesure, au collaborateur du fournisseur de services, au distributeur de logiciel, au spécialiste en sécurité informatique, à l'opérateur de télécommunications ... En respect du droit au silence et du droit de ne pas contribuer à sa propre incrimination, l'obligation de collaboration ne pourra toutefois être imposée ni à l'inculpé ni à ses ascendants, descendants, frères, sœurs, conjoints et alliés (276). Elle ne pourra pas non plus être imposée, bien que le texte ne le précise pas, aux personnes astreintes au secret professionnel (277). Ces dispenses ne concernent toutefois que l'obligation d'intervention sur le système informatique, et non pas l'obligation de communiquer des informations relatives au fonctionnement du système (278).

En ce qui concerne l'aide demandée, celle-ci sera de nature technique et soumise à une obligation de moyens (279). Il appartiendra au juge d'instruction de prendre une ordonnance précisant la mission ainsi que les circonstances justifiant la mesure (280).

Les personnes appelées à collaborer seront tenues au secret professionnel pour leur participation à la mesure (281).

En vue de garantir l'effectivité de la mesure, le refus de collaborer a été érigé en infraction particulière passible d'une peine allant de six

(276) Tels que repris à l'art. 156 du C. instr. crim.

(277) C. Meunier, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *op. cit.*, p. 685. Aux termes de l'exposé des motifs, les titulaires du secret sont soumis au même régime que s'ils étaient appelés à témoigner en justice : ils ont donc la faculté de collaborer à la recherche mais ne peuvent y être contraints.

(278) C. instr. crim., art. 88*quater*, §2, al. 2 *in fine*.

(279) C. instr. crim., art. 88*quater*, §2, al. 1 *in fine*.

(280) Cette mesure ne peut être ordonnée que si elle est nécessaire, p. ex. parce que le système informatique à examiner est trop complexe ou parce qu'il n'y a pas suffisamment d'agents qualifiés sur place (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 27).

(281) Sous peine de sanction pénale telle que prévue à l'art. 458 du C. pén.

mois à un an de prison (et donc susceptible de donner lieu à la délivrance d'un mandat d'arrêt (282)) et d'une amende comprise entre 26 et 20.000 EUR. Les mêmes peines peuvent être infligées aux personnes requises qui feindraient de ne pouvoir accéder aux fichiers ou qui supprimeraient volontairement les informations pertinentes (283).

Il est à noter que selon la loi, l'État est responsable civilement des dommages causés involontairement par la personne dont la collaboration a été requise (284).

85. Le refus de collaboration dans le cadre de l'interception de communications et télécommunications privées. Pareille réquisition peut être faite pour l'interception de communications et télécommunications privées (C. instr. crim., art. 90*quater*, §4). Le juge d'instruction peut en effet ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la communication qui est ou a été transmise.

Les personnes visées par cette disposition sont certes les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications (déjà visés au §2 de l'art. 90*quater* du C. instr. crim.), mais aussi toutes les autres personnes ayant des connaissances particulières utiles à l'instruction, comme les services de cryptographie, d'accès à l'internet, de messagerie ou de transport, notamment (285).

Le juge d'instruction peut ordonner à toutes ces personnes de rendre accessible le contenu de la télécommunication dans la forme qu'il aura demandée.

Dans les mêmes conditions que celles prévues à l'article 88*quater*, le refus de prêter son concours aux services d'enquête est susceptible d'entraîner les mêmes peines (*cf. supra*).

(282) L. 20 juillet 1990 relative à la détention préventive, art. 16, §1er, al. 1er.

(283) *Doc. parl.*, Sén., sess. ord. 1999-2000, n° 2-392/3, pp. 63 et 69.

(284) Les dommages volontaires ne pourront être mis à charge de l'État (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 50 0213/001, p. 28). Ils pourront, le cas échéant, faire l'objet d'une demande d'indemnisation par la voie civile à l'encontre du responsable du dommage.

(285) Y. POULLET, «À propos du projet de loi dit n° 214. La lutte contre la cybercriminalité dans le cyberespace à l'épreuve du principe de la régularité des preuves», in *Liber Amicorum Jean du Jardin*, Deurne, Kluwer, 2001, p. 22.

Section 2. – Criminalité informatique aspécifique

86. Criminalité aspécifique – Notion. La criminalité informatique aspécifique ne se distinguant de la criminalité de droit commun que par son mode d'exécution, la présente contribution se limitera à rappeler succinctement différentes bases légales pertinentes en la matière et à mettre en exergue certaines questions particulières nées de l'application du droit pénal commun à ces infractions lorsqu'elles sont commises au moyen d'un système informatique.

§ 1. – Atteintes à la vie privée

87. Bases légales. Différentes dispositions protègent pénalement la vie privée, en ce compris dans l'univers numérique. Parmi celles-ci, et de manière non exhaustive, relevons les dispositions suivantes.

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (286) contient différentes dispositions pénales sanctionnant le non-respect des obligations imposées aux responsables de traitements de données à caractère personnel. L'article 314*bis* du Code pénal (287) sanctionne l'écoute, la prise de connaissance ou l'enregistrement volontaire, à l'aide d'un appareil quelconque, de communications ou télécommunications privées par une personne qui n'y prend pas part et sans le consentement de tous les participants. Cette disposition vise la prise de connaissance du contenu d'une télécommunication (288) pendant sa transmission. Tous les procédés de communication privée sont visés : mail, SMS ... (289). Les travaux préparatoires de la loi précisent par ailleurs que les données transmises via les réseaux, des ordinateurs ou l'internet sont visées (290). La Commission de la protection de la vie privée a estimé

(286) *M.B.*, 18 mars 1993. Pour une étude de l'application de la loi du 8 décembre 1992 à la criminalité informatique, voy. D. DE BOT, «Traitement de données à caractère personnel et criminalité informatique : *Deus ex machina* et/ou épée de Damoclès?», *A.P.2-T*, n° 6, pp. 8-16.

(287) Introduit par la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications, *M.B.*, 24 janvier 1995.

(288) Et non pas des données, comme l'a précisé la Cour du travail de Gand (C. trav. Gand, 4 avril 2001, *J.T.T.*, 200, p. 49). Dans le même sens, C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100, note P. VAN EECKE et B. OOMS, «De controle van e-mail- en internetgebruik door de werkgever in België : ambiguïteit in de rechtspraak». Selon ces deux juridictions, les SMS et les messages e-mail relèvent de la notion de données en matière de télécommunications. Les travaux préparatoires de la loi précisent d'ailleurs que l'employeur a la possibilité de relever les numéros de téléphone appelés par le travailleur (*Ann. parl.*, Sén., sess. ord. 1992-1993, n° 843/2, p. 42).

(289) M. CRANSHOFF, «L'employeur peut-il contrôler les e-mails envoyés par ses collaborateurs?», *Chroniques sociales de HDP secrétariat social*, www.hdp.be.

(290) *Ann. parl.*, Sén., sess. ord. 1992-1993, n° 843/2, p. 10.

que cette disposition n'était pas d'application à la consultation de données stockées (291). Échappe donc à la répression de l'article 314*bis*, la consultation d'e-mails reçus par le destinataire ou la consultation de SMS dans la mémoire d'un GSM (292). Pareille situation ne tombe pas non plus sous le coup de l'article 460 du Code pénal relatif au secret des lettres. Cette disposition assortit en effet de sanctions pénales la suppression d'une lettre confiée à un opérateur postal ou l'ouverture d'une telle lettre pour en violer le secret. Il nous apparaît qu'en raison de la définition de la lettre (en tant qu'elle est confiée à un opérateur postal), et en vertu du principe d'interprétation stricte du droit pénal, cette disposition ne pourrait trouver à s'appliquer lors de la prise de connaissance du contenu d'un e-mail ou d'un SMS arrivé à son destinataire (293).

La loi du 13 juin 2005 relative aux communications électroniques (294) a remplacé une partie de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, et notamment son article 109*ter*D, qui érigeait en principe l'interdiction de prendre connaissance de données transmises par voie de télécommunications. L'article 124 de la loi du 13 juin 2005 interdit dorénavant à quiconque de prendre intentionnellement connaissance de l'existence d'une information transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ou d'identifier les personnes concernées par la transmission de l'information et de son contenu. La notion de communication électronique est définie comme étant la transmission de

(291) Commission vie privée, Avis n° 10/2000 du 3 avril 2000.

(292) À ce propos, on relèvera toutefois que la Cour du travail d'Anvers a considéré que les dispositions de la convention collective de travail n° 81 du 26 avril 2002 selon lesquelles l'employeur peut prendre connaissance des courriels ayant un caractère professionnel étaient incompatibles avec l'art. 8 de la Convention européenne des droits de l'homme, l'art. 314*bis* du C. pén., l'art. 109*ter* de la loi du 21 mars 1991 relative aux entreprises publiques autonomes et la loi du 8 déc. 1992 sur le traitement des données à caractère personnel (C. trav. Anvers (2 ch.), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146). La Cour du travail de Gand a, quant à elle, considéré que l'art. 314*bis* du C. pén. n'était pas applicable à l'acquisition d'un *view-access log* permettant de vérifier les sites internet qu'une personne a consultés. Et que l'art. 109*ter*D, 3°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques n'était pas applicable au contrôle exercé au sein de l'entreprise sur la consultation de l'internet (C. trav. Gand, 9 mai 2005, *Computerr.*, 2006, p. 107, note P. Van Eecke et B. Ooms; *Juristenkrant*, 2005, n° 117, p. 1; *Chron. D.S.*, 2006, p. 158).

(293) Dans le même sens, not. : O. Rijckaert, «Le contrôle de l'usage d'internet et de l'e-mail sur le lieu de travail au regard de la convention collective de travail n° 81 du 26 avril 2002», *Bulletin social du guide social permanent*, Diegem, Kluwer, 2002, p. 54; C. trav. Liège, 25 avril 2002, *J.L.M.B.*, 2003, p. 17. En France, le Tribunal de grande instance de Paris avait décidé, le 9 novembre 2000, que «l'envoi de messages électroniques de personne à personne est considéré comme de la correspondance privée» (T.G.I. Paris, 9 novembre 2000). Mais la définition du Code pénal français se prête mieux à une adaptation au courrier électronique.

(294) *M.B.*, 20 juin 2005.

signaux autres que ceux de radiodiffusion et de télévision (295). Les données analogiques ou numériques sont donc visées (296).

Enfin, l'article 433*bis* du Code pénal sanctionne la publication par tout moyen, en ce compris l'internet, du compte-rendu des débats tenus devant une juridiction de la jeunesse.

§ 2. – Utilisation abusive de l'infrastructure publique de télécommunications

I. – *Harcèlement par communications électroniques et dommage*

88. Harcèlement «téléphonique». Jusqu'il y a peu, le harcèlement qualifié de téléphonique était incriminé par l'article 114, §8, 2°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Cette disposition, qui a été abrogée par la loi du 13 juin 2005 relative aux communications électroniques, disposait que : «Est punie d'une amende de 500 à 50.000 (francs) maximum et d'un emprisonnement d'un à quatre ans ou d'une de ces peines seulement : (...) 2° la personne qui utilise un réseau ou un service de télécommunications ou d'autres moyens de télécommunications afin d'importuner son correspondant ou de provoquer des dommages».

Depuis l'abrogation de cette disposition, le harcèlement par voie de télécommunications est réprimé sur la base de l'article 145, §3, 2°, de la loi relative aux communications électroniques (297), rédigé comme suit : «Est punie d'une amende de 500 a 50.000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement : (...) 2° la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages».

Cette disposition, dont il convient de souligner la largesse des termes, recouvre dorénavant tant le harcèlement téléphonique que d'autres formes de harcèlement commis par l'intermédiaire de communications électroniques (298). On pense notamment au *spamming* (technique consistant

(295) L. 13 juin 2005, art. 2.

(296) S. van Wassenhove, «Le respect de la vie privée dans l'usage des nouvelles technologies», in *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. Jeune Barreau, 2005, p. 155.

(297) Tel qu'inséré par la loi du 13 juin 2005.

(298) Sous l'empire de l'ancienne loi, un homme avait répandu sa haine raciale dans le cadre de forums de discussions gérés par la société Infonie. Après que les modérateurs du site l'aient repéré et l'aient enjoint à cesser son comportement culpeux, celui-ci les avait insultés. La société Infonie avait fini par porter plainte avec constitution de partie civile. Le tribunal l'avait condamné pour racisme mais avait également considéré

en l'envoi de communications commerciales non sollicitées), à l'envoi répété de SMS ou de mails dans le but de nuire à la tranquillité du destinataire (299) ...

On relèvera, bien que le texte ne le prévoie pas explicitement, que le harcèlement ne pourra se fonder sur un fait unique. C'est en tous cas, à notre estime, le sens dans lequel il convient d'interpréter le verbe «importuner», conformément à ce qu'a récemment décidé la Cour de cassation à propos du harcèlement fondé sur l'article 442*bis* du Code pénal (300).

89. Dommage par communications électroniques. Outre le harcèlement, la loi vise également l'utilisation d'un réseau ou d'un service de télécommunications électroniques afin de provoquer des dommages. Cette infraction ne se confond pas avec le sabotage informatique, puisqu'ainsi que cela a déjà été indiqué *supra*, le sabotage informatique ne suppose pas qu'un dommage ait été causé à des données ou à un système informatique (le dommage n'étant, le cas échéant, qu'une circonstance aggravante de l'infraction). Par ailleurs, l'hypothèse visée par l'article 145, §3, 2°, de la loi du 13 juin 2005 ne se limite pas aux cas où des données ont été introduites, modifiées ou effacées dans un système informatique et vise, beaucoup plus largement, tous les cas où des dommages auraient été causés par l'utilisation d'un réseau ou d'un service de télécommunications électroniques. Le cas échéant, de mêmes faits pourraient donc donner lieu à des poursuites concurrentes sur la base de ces préventions (301).

II. – *Réalisation frauduleuse de communications électroniques*

90. Réalisation frauduleuse de communications électroniques. L'article 145, §3, 1°, de la loi du 13 juin 2005 punit des mêmes peines que celles prévues pour le harcèlement la personne qui réalise frauduleusement des communications électroniques au moyen

que «l'utilisation frauduleuse de l'infrastructure de télécommunications pour tenir des propos xénophobes et l'utilisation des abonnements à un fournisseur d'accès internet de tiers pour se connecter à internet à leur insu, sont punissables par l'article 114, §8 de la loi du 21 mars 1991. Des communications via internet sont des 'appels malicieux' visés par cet article» (Corr. Bruxelles, 15 janvier 2002, *R.D.T.I.*, 2002, n° 13, pp. 73-75). Ces agissements tomberaient aujourd'hui sous le coup de l'art. 145 de la loi du 13 juin 2005.

(299) Pourrait égal. tomber sous le coup de la disposition, l'ouverture répétitive de fenêtres non sollicitées lors de la consultation de pages web (*pop-up*).

(300) Cass., 21 février 2007, R.G. n° P.06.1415.F, *www.cass.be*.

(301) En ce cas, sous réserve d'application de la seule loi particulière, ces infractions viendront en concours idéal.

d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite. Cela vise notamment les communications téléphoniques passées au départ du téléphone d'un tiers sans son autorisation, mais aussi, vu la largesse des termes, l'abus de connexion internet (notamment en cas de connexion sans fil), déjà visé par l'article 550*bis* du Code pénal (*cf. supra*).

§ 3. – Racisme, xénophobie, révisionnisme

91. Principe de liberté d'expression et limitations. La liberté d'expression est un des fondements essentiels d'une société démocratique, qui doit être respectée lorsque ce qu'elle véhicule est accueilli favorablement mais également, sous réserve, lorsqu'elle fait écho d'idées ou d'opinions qui dérangent, heurtent, choquent ou inquiètent (302). Elle doit donc être entendue largement, ce qui ne la dispense toutefois pas de certaines limitations qui doivent être appliquées à toutes les formes de communications, en ce compris les communications électroniques.

Ainsi, bien que l'internet soit dominé, depuis sa création, par un mythe de la liberté, il n'en demeure pas moins que l'expression par ce mode particulier de communication (web, blog, chat ...) reste soumis à ces limitations. L'article 10, alinéa 2, de la Convention européenne des Droits de l'Homme prévoit en effet que «L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions, prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité du territoire ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire».

Les limites à la liberté d'expression doivent donc respecter différentes conditions qui doivent être prévues par une loi (au sens large) et être justifiées par un des motifs limitativement énumérés par la Convention européenne des Droits de l'Homme (dans le respect du principe de proportionnalité).

(302) C.E.D.H., *Thoma c. Luxembourg*, arrêt du 29 mars 2001, §44.

92. Racisme et révisionnisme. La loi du 30 juillet 1981 (dite «loi Moureaux») est de celles-là (303). Elle incrimine non seulement les actes directs de discrimination raciale, mais également l'incitation à la discrimination raciale (304), laquelle doit être entendue comme étant «la volonté manifeste de conduire un tiers à accomplir de tels comportements» (305). De même, la loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste pendant la seconde guerre mondiale sanctionne d'un emprisonnement de huit jours à un an et d'une amende de 26 à 5.000 EUR celui qui, dans l'une des circonstances visées à l'article 444 du Code pénal, nie, minimise grossièrement, cherche à justifier ou approuve le génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale (306).

Ces lois soumettent la répression à une condition essentielle de publicité : les actes incriminés doivent avoir été posés dans l'une des hypothèses visées à l'article 444 du Code pénal. Il faut donc que les actes aient été commis «soit dans des réunions ou lieux publics, soit en présence de plusieurs individus, dans un lieu non public, mais ouvert à un certain nombre de personnes ayant le droit de s'y assembler ou de le fréquenter, soit dans un lieu quelconque, en présence de la personne offensée et devant témoins, soit par des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public, soit enfin par des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes».

Dans le cadre de la criminalité informatique, et compte tenu de cette exigence, l'expression de pensées racistes, xénophobes ou négationnistes soulève principalement deux questions : la condition de publicité est-elle remplie lorsque les propos ont été diffusés sur une page web ou dans

(303) De même, le Protocole additionnel de la Convention cybercriminalité vise à prévenir le racisme et la xénophobie sur internet par la criminalisation de la diffusion de matériel raciste et xénophobe via les systèmes informatiques, ainsi que les menaces et insultes racistes, le négationnisme, le révisionnisme ou la justification des crimes contre l'Humanité. L'art. 2 de ce Protocole définit le matériel raciste ou xénophobe comme étant «tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes», ce qui constitue une définition plus large que celle de la loi belge.

(304) L. 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, *M.B.*, 8 août 1981.

(305) *Doc. parl.*, Ch. repr., sess. ord. 1980-1981, n° 594/2, p. 15.

(306) L. 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste pendant la seconde guerre mondiale, *M.B.*, 30 mars 1995, et *err.*, *M.B.*, 22 avril 1995.

le cadre d'un forum de discussions et, dans l'affirmative, peut-on parler de délit de presse ?

I. – *Publicité au sens de l'article 444 du Code pénal*

93. Publicité des sites web et forums de discussion. Différentes juridictions ayant eu à connaître de cas de racisme ou de xénophobie commis par le biais de sites web ou de forums de discussion ont déjà considéré que la condition de publicité était remplie lorsque des propos racistes ou xénophobes avaient été tenus par le biais de tels médias. Ainsi, notamment, la Cour d'appel de Bruxelles avait considéré que : «il ne peut être sérieusement contesté que les messages e-mails attribués au prévenu sont des écrits (imprimés ou non), si pas exposés au regard du public, à tout le moins adressés ou communiqués à plusieurs personnes, en l'espèce à toute personne consultant le forum de discussions sur le réseau internet; qu'il s'ensuit que l'infraction, à la supposer établie, a bien été commise dans l'une des circonstances indiquées à l'article 444 du Code pénal» (307). Nous nous rangeons à cette opinion.

II. – *Délit de presse et internet*

94. Délit de presse – Notion. Le délit de presse est l'infraction réprimant les abus commis dans l'exercice de la liberté de la presse (308). Il peut consister en toute infraction (calomnie, diffamation, incitation à la discrimination raciale ...) véhiculant la manifestation d'une pensée ou d'une opinion abusive, illicite ou coupable commise par la voie de la presse. Il s'agit donc d'une infraction ordinaire caractérisée par son mode d'exécution (un écrit imprimé, reproduit et publié) qui ne se limite pas aux infractions visées par le décret du 20 juillet 1831 sur la presse (309). Le délit de presse est soumis à un régime répressif dit de faveur, puisqu'il ne peut être jugé que par une Cour d'assises, à l'exception des délits de presse inspirés par le racisme ou la xénophobie (310).

(307) Bruxelles, 27 juin 2000, *A. & M.*, 2001, p. 142, note D. VOORHOOF, «Aanzet tot racisme via Internet – Drukpersmisdrijf of geen drukpersmisdrijf : de correctionele rechtbank is bevoegd!»; *Rev. dr. étr.*, 2000, p. 321. C'est égal. en ce sens qu'avait tranché le Tribunal correctionnel de Bruxelles (Corr. Bruxelles, 15 janvier 2002, *R.D.T.I.*, 2002, n° 13, pp. 73-75). Dans le même sens, T.G.I. Paris, 26 février 2002, *R.D.T.I.*, 2002, n° 13, p. 76, note P. VALCKE et C. UYTTENDAELE.

(308) Il n'existe pas de définition légale du délit de presse. Sur la notion, voy. F. TULKENS et M. VAN de KERCHOVE, *Introduction au droit pénal*, 6e éd., *op. cit.*, pp. 255 et s.; C. HENNAU et J. VERHAEGEN, *Droit pénal général*, 2e éd., *op. cit.*, pp. 58 et s.; S. HOEBEKE et B. MOUFFE, *Le droit de la presse*, Bruxelles, Bruylant, 2000, pp. 82 et s.

(309) C. HENNAU et J. VERHAEGEN, *Droit pénal général*, 2e éd., *op. cit.*, pp. 65 et s.

(310) Art. 25 et 150 de la Constitution, Décrets des 19 et 20 juillet 1831.

95. Délit de presse et internet. Traditionnellement, la Cour de cassation a, par une jurisprudence constante, refusé d'étendre la notion de délit de presse aux délits commis par le biais d'émissions télévisées ou radiodiffusées, au motif, essentiellement, que les émissions de télévision ou de télédistribution ne pouvaient être considérées comme des modes d'expression par des écrits imprimés (311). Cette jurisprudence amènerait certainement la Cour à exclure du délit de presse la presse électronique, et donc toute diffusion de messages à l'intermédiaire de l'internet (312). Car, si elle n'a pas encore été amenée à se prononcer explicitement sur la question, elle a toutefois considéré, de façon plus générale en matière de délits de presse, que «l'évolution technologique (...) incite à privilégier une approche prudente face aux défis juridiques et au bouleversement de l'ordonnance juridique que provoquent l'émergence de nouveaux médias et la convergence technologique des médias dont les contours juridiques ne sont pas encore parfaitement arrêtés» (313).

Selon la Cour constitutionnelle toutefois, laquelle avait été appelée à se prononcer dans un tout autre contexte, à savoir la conformité à la Constitution de la loi sur la protection des sources journalistiques, il semble que l'internet puisse être assimilé à un média de presse (314).

Quoi qu'il en soit, différentes juridictions de fond ont déjà décidé que des infractions commises via l'internet devaient être considérées comme des délits de presse (315) et une majeure partie de la doctrine, derrière

(311) Cass., 2 mars 1964, *Pas.*, 1964, I, p. 697; Cass., 9 décembre 1981, *Pas.*, 1982, I, p. 482; Cass., 2 juin 2006, sur concl. conf. av. gén. DE KOSTER, *A. & M.*, 2006, p. 355; *J.L.M.B.*, 2006, p. 1403, obs. F. JONGEN. Dans le cadre de ce dernier arrêt, la Cour avait considéré que la presse se résumait à la publication «d'écrits, imprimés ou reproduits par voie de tirages répétés, suivant un procédé analogue à celui de l'imprimerie». Sur cette question, voy. égal. D. DE BELLESCIZE et L. FRANCESCHINI, *Droit de la communication*, Paris, P.U.F., 2005, pp. 435 et s.

(312) Dans le même sens, Y. POULLET, «La lutte contre le racisme et la xénophobie sur internet», *J.T.*, 2006, p. 404.

(313) Cass., 2 juin 2006, *op. cit.*

(314) C. const., 7 juin 2006, n° 91/2006, *Arr. C.A.*, 2006, p. 1061; *www.arbitrage.be*; *A. & M.*, 2006 p. 295, note; *M.B.*, 23 juin 2006, p. 32141; *Juristenkrant*, 2006, n° 132, p. 17; *Mediaforum* (Pays-Bas), 2006, n^os^ 7-8, p. 235; *NjW*, 2006, p. 645, note P. VALCKE, E. LIEVENS et E. WERKERS; *R.W.*, 2006-2007, p. 1349, note E. BREWAEYS, «Recente rechtspraak van het Arbitragehof over persvrijheid».

(315) Corr. Bruxelles, 22 décembre 1999, *A. & M.*, 2000, p. 134. Le même raisonnement a présidé à l'ordonnance du 2 mars 2000 rendue dans le cadre d'une procédure en référé relative à des propos diffamatoires figurant à la fois sur un site personnel et dans un forum de discussions. Le président du Tribunal de première instance de Bruxelles avait en effet décidé qu'il s'agissait d'un délit de presse devant être considéré comme un délit continu tant que le texte litigieux restait aisément accessible à toute personne naviguant sur le net (Civ. Bruxelles (réf.), 2 mars 2000, *A. & M.*, 2001, p. 147, note M. ISGOUR; *J.T.*, 2002, p. 113, note E. WÉRY). Voy. égal., dans le même sens, Civ. Bruxelles (réf.), 19 février 2004, *R.D.T.I.*, 2005, n° 21, p. 75, note K. LEMMENS, «Les publications sur la toile peuvent-elles constituer des délits de presse?»; Corr. Bruxelles, 7 novembre 2000, *A.J.T.*, 2000-2001, p. 497, note D. VOORHOOF, «Verspreider van revisionistisch tijdschrift correctioneel veroordeeld wegens drukpersmisdrijf ingegeven door racisme of xenofobie»; *A. & M.*, 2000, p. 473; *Rev. dr. étr.*, 2000, p. 665, note B. RENAULD, «Un délit de presse négationniste condamné par le tribunal correctionnel». Ce dernier jugement a été confirmé en appel : Bruxelles (11^e^ ch.), 27 juin 2000, *A. & M.*, 2001, p. 142, note D. VOORHOOF, «Aanzet tot racisme via Internet – Drukpersmisdrijf of geen drukpersmisdrijf : de correctionele rechtbank is bevoegd!»; *Rev. dr. étr.*, 2000, p. 321; Corr. Mons, 13 février 2007, inédit. Y. POULLET, «La lutte contre le racisme et la xénophobie sur internet», *op. cit.*, p. 405.

(316) M. ISGOUR, «Le délit de presse sur Internet a-t-il un caractère continu?», *A. & M.*, 2001, p. 156; Th. VERBIEST, «La presse électronique. Droit d'auteur, délit de presse, responsabilité en cascade, droit de réponse, racisme, révisionnisme», *A. & M.*, 2000, pp. 69-79; D. VOORHOOF, note sous Corr. Bruxelles, 22 décembre 1999, *A. & M.*, 2000, p. 134; S. HOEBEKE et B. MOUFFE, *Le droit de la presse*, *op. cit.*, pp. 24 et s.; A. STROWEL, «La lutte contre les activités liberticides sur internet», in *Pas de liberté pour les ennemis de la liberté*, Bruxelles, Bruylant, 2000, p. 411. *Contra* : T. DE PESSEMIER, *Vrijheid van expressie en informatie op het internet*, Gent, Academia Press, 1997, pp. 94 et 96.

(317) Le délit de presse «traditionnel» est un délit instantané consommé par la première mise à disposition du public.

(318) Le législateur français a choisi, dans le cadre de la loi française pour la confiance dans l'économie numérique du 21 juin 2004 (L.C.E.N.), d'assimiler l'internet à un médium de presse pour «toute transmission sur demande individuelle de données numériques n'ayant pas un caractère de correspondance privée par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur».

(319) Cass. fr., 30 janvier 2001, disponible en ligne : http://www.droit-technologie.org/jurisprudences/cass_france_300101.pdf; Cass. fr., 16 octobre 2001, *R.E.D.C.*, 2001, p. 94, note S. CHILLON; disponible en ligne : http://www.courdecassation.fr/agenda/arrets/arrets/00-85728.htm).

(320) La Cour d'appel de Paris avait décidé, le 15 décembre 1999, que la diffusion sur l'internet était un acte de publication continue.

laquelle nous nous rangeons, admet que des délits de presse puissent être commis sur le web ou dans un forum de discussion (316).

96. Prescription du délit de presse sur l'internet. En guise de question sous-jacente, la question de la prescription du délit de presse lorsqu'il était commis en ligne a suscité de nombreux débats. Étant donné que la publication des informations s'étend aussi longtemps que celles-ci restent en ligne, faut-il considérer que le délai de prescription prend cours au jour de la publication des données litigieuses ou au jour de leur retrait? En d'autres termes, le délit de presse commis sur l'internet est-il un délit instantané (317) ou continu? C'est en France que la controverse connut le plus grand écho en raison du fait que la législation française soumet sans ambiguïté les délits commis sur l'internet au régime du délit de presse (318). Par deux arrêts distincts, la Cour de cassation de France a considéré que les délits de presse sur l'internet étaient des délits instantanés (319). Elle a ramené le point de départ de la prescription «à la date du premier acte de publication» ou «à la date à laquelle le message a été mis pour la première fois à disposition des utilisateurs». Ce faisant, elle s'est opposée à différentes juridictions de fond qui avaient considéré, au contraire, qu'il s'agissait de délits continus, la prescription ne commençant à courir qu'à partir du moment où la publication en ligne prenait fin (320). Ces décisions avaient été diversement appréciées par la

doctrine française (321). En Belgique, la doctrine a majoritairement conclu au caractère instantané du délit de presse commis sur l'internet (322).

§ 4. – Corruption de la jeunesse – Outrages aux bonnes mœurs

97. Bases légales supranationales. Différents textes internationaux sanctionnent la pornographie enfantine. La Convention internationale des droits de l'enfant prévoit, en son article 34, l'obligation pour les États de protéger les enfants contre les incitations ou la contrainte à se livrer à une activité sexuelle illégale, d'empêcher l'exploitation à des fins de prostitution ou autres pratiques sexuelles illégales et l'exploitation aux fins de la production de spectacle ou de matériel de caractère pornographique. Un Protocole facultatif à cette Convention internationale dénonce spécifiquement les usages pervers de l'internet en la matière.

Au niveau du Conseil de l'Europe, la Convention sur l'exercice des droits de l'enfant du 25 janvier 1996 contient des dispositions similaires. De même, la Convention sur la cybercriminalité vise spécifiquement la répression de la pédopornographie.

98. Incrimination de la pédopornographie en droit interne. En droit interne, les articles 379 et suivants du Code pénal sont applicables à l'exploitation de la pédopornographie sur l'internet. Plus particulièrement, l'article 383*bis*, § 1er, sanctionne d'une peine de réclusion de cinq ans à dix ans et d'une amende de 500 à 10.000 EUR l'exposition, la vente, la location, la distribution, la diffusion ou la remise d'emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique impliquant ou présentant des mineurs. Le § 2 de cette même disposition vise la possession desdits supports et y attache un emprisonnement d'un mois à un an

(321) Voy. not. B. Ader, «Évolution de la notion de publication de la presse écrite à internet», *Légipresse*, 1999, n° 165, pp. 123 et s.; B. Ader, «La publication sur internet de messages délictueux est un délit continu», note sous Paris, 15 décembre 1999, *Légipresse*, 2000, n° 169, p. 39; P. Blanchetier, «Point de départ du délai de prescription des délits de presse sur internet : vers une solution libertaire et contraire au bon sens», *D.-S.*, 2001, pp. 2056-2058; P.-Y. Gautier, «De la prescription des infractions commises sur l'internet ... et dans le monde physique», *D.-S.*, 2002, pp. 1852-1855; D. Rebut, «Prescription des délits de presse sur l'internet : le régime de la loi de 1881», *Légipresse*, 2001, n° 182, pp. 63-67; C. Rojinsky, note sous Paris, 23 juin 2000, *Légipresse*, n° 176, p. 182.

(322) M. Isgour, «Le délit de presse sur Internet a-t-il un caractère continu?», *op. cit.*, p. 157, G. Vogel., *Droit de la presse*, Luxembourg, Éditions Promoculture, 2000, p. 198; S. Hoebeke et B. Mouffe, *Le droit de la presse*, *op. cit.*, p. 625.

et une amende de cent à mille euros (323). La notion de possession n'implique bien sûr pas que les fichiers incriminés aient fait l'objet d'une matérialisation quelconque (impression, projection ...). Elle se suffit d'une simple disposition. La Cour de cassation a même considéré que par exposer et diffuser au sens de l'article 383*bis*, § 1er, du Code pénal, il fallait également entendre l'établissement sur un site web d'hyperliens vers des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des attitudes ou des actes sexuels à caractère pornographique impliquant ou présentant des mineurs (324). Tombe donc sous le coup de la disposition, le seul établissement d'hyperliens vers un contenu pédopornographique (325). Cette approche nous semble correcte, car à défaut de considérer le renvoi par liens hypertextes vers du contenu illicite comme étant déjà une forme de possession, il eût été aisé, pour les exploitants de pédopornographie, de s'assurer une impunité pénale simplement en se retranchant derrière l'argument fallacieux qui aurait consisté à dire qu'ils n'étaient pas eux-mêmes possesseurs des fichiers litigieux.

À ce propos, on notera que la loi soumet la possession de fichiers pédopornographiques à la condition que leur auteur les ait possédés sciemment. Il faut donc que la partie poursuivante établisse que celui-ci avait agi avec dol général. Il s'en déduit, *a contrario*, que le téléchargement involontaire de fichiers contenant des supports visuels à caractère pédopornographique ne tombe pas sous le coup de la loi. Ainsi, l'enregistrement dans les fichiers temporaires de tels documents, lorsqu'il aura été le fait de programmes malicieux ayant pour effet de télécharger, à l'insu et parfois même contre la volonté de l'utilisateur, ne tombera pas sous le coup de la loi pénale, sauf à démontrer que cet enregistrement avait été fait volontairement (dans le but, sans doute, de se prévaloir d'une ignorance feinte) (326).

(323) Sur cette problématique, voy. not. O. Leroux, «La corruption de la jeunesse et les outrages publics aux bonnes mœurs par courrier électronique (courriel, SMS, MMS)», *R.D.T.I.*, 2003, n° 17, pp. 13-24.

(324) Cass., 3 février 2004, *Pas.*, 2004, p. 200; *www.cass.be*; *A. & M.*, 2005, p. 259, note; *Computerr.* (Pays-Bas), 2004, n° 5, p. 242 et note S. De Schrijver; *Juristenkrant*, 2004, n° 85, p. 6; *R.D.T.I.*, 2004, n° 19, pp. 51-59, note F. de Patoul et I Vereecken, «La responsabilité des intermédiaires de l'internet : première application de la loi belge».

(325) «L'exploitant d'un site web sur lequel se trouve une longue liste d'hyperliens vers des sites web avec des images pédopornographiques, ne peut pas être traité de la même manière qu'un fournisseur de services internet, vu que celui-ci fournit l'accès – généralement payant – à ses abonnés à l'internet entier et global pour rechercher des sujets divers, et par conséquent n'organise pas une offre visée sur d'autres sites web avec un sujet commun. L'exploitant d'un site web peut être tenu pour responsable du contenu concret des sites web vers lesquels les liens réfèrent, si son engagement apparaît par le fait que les hyperliens sont assemblés et offerts sur son site et qu'il en est conscient» (Anvers, 7 octobre 2003, *A. & M.*, 2004, p. 164, note E. Lievens, «Aansprakelijkheid voor hyperlinks : linke regeling?»; *Computerr.* (Pays-Bas), 2004, n° 2, p. 85, note C. De Preter, «Aansprakelijkheid voor (het hosten van) links»).

(326) *Cf. supra*, Cass. fr., 5 janvier 2005.

§ 5. – Atteintes à la propriété intellectuelle

99. Contrefaçon. Les articles 80 et suivants de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins (327) sanctionnent l'atteinte méchante ou frauduleuse portée au droit d'auteur et aux droits voisins d'une peine d'amende comprise entre 100 et 100.000 EUR. En cas de récidive, une peine d'emprisonnement de trois mois à deux ans peut également être prononcée.

La définition de la disposition est large et englobe toute atteinte au droit d'auteur ou à un droit voisin, qu'il s'agisse du droit patrimonial (droit de reproduction, en ce compris le droit de distribution ou le droit à rémunération pour copie privée, et droit de communication au public) ou du droit moral (328).

La mise à disposition en ligne (*upload*) au public d'une œuvre protégée par le droit d'auteur est en principe interdite, sauf accord du titulaire du droit. Le téléchargement (*download*) d'une telle œuvre ne l'est pas nécessairement (329).

100. Protection des programmes d'ordinateur. On notera encore que la loi du 30 juin 1994 concernant la protection juridique des programmes d'ordinateur (330) sanctionne particulièrement la détention d'une copie illicite d'un programme d'ordinateur, ainsi que la mise en circulation ou la détention de moyens ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation des dispositifs techniques qui protègent un programme d'ordinateur. L'article 2 de cette loi prévoit qu'un programme est protégé s'il est original, soit une création intellectuelle propre à son auteur. Et en ce qui concerne l'incrimination de la détention de systèmes de neutralisation de dispositifs de protection d'un programme d'ordinateur, si cette incrimination est à rapprocher du §5 de l'article 550*bis* du Code pénal qui vise les *hackertools*, elle ne s'y identifie pas, dans la mesure où les *hackertools* sont des dispositifs destinés à faciliter l'accès à un système informatique, tandis que les moyens visés par la présente loi sont ceux destinés à neutraliser des dispositifs techniques de protection d'un programme (*cf. supra*).

(327) *M.B.*, 27 juillet 1994.

(328) F. de Visscher et B. Michaux, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, p. 532.

(329) Voy. not. sur cette question, Civ. Bruxelles (prés.), 26 novembre 2004, *A. & M.*, 2005, p. 49, note L. Van Bunnen; *Computerr.* (Pays-Bas), 2005, n° 2, p. 65, note F. Petillon; *I.R.D.I.*, 2005, p. 41; *Ing.-Cons.*, 2004, p. 560; *J.T.*, 2005, p. 165, note I. Schmitz; *Juristenkrant*, 2005, n° 103, p. 5, note J. Deene; *NjW*, 2005, p. 743, note J. Deene; *R.D.T.I.*, 2005, n° 21, p. 89, note E. Montero et Y. Cool.

(330) Loi transposant en droit belge la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur, *M.B.*, 27 juillet 1994.

101. Protection des bases de données. On relèvera enfin la loi du 31 août 1998 concernant la protection juridique des bases de données (331), qui sanctionne notamment toute atteinte méchante ou frauduleuse portée au droit des producteurs de bases de données ainsi que toute application méchante ou frauduleuse du nom d'un producteur de bases de données ou de tout signe distinctif adopté par lui pour désigner sa prestation.

Bibliographie

De Hert P. et Lichtenstein G., «De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht», *C.B.R. (Jaarboek)*, 2003, Anvers, Maklu, pp. 345-420.

de Villenfagne F. et Dusollier S., «La Belgique sort enfin ses armes contre la criminalité informatique : à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *A&M*, 2001.

Evrard S., «La loi du 28 novembre 2000 relative à la criminalité informatique», *J.T.*, 2001, pp. 241 et s.

Laureys T., *Informatica criminaliteit*, Mys & Breesch, 2001, 117 p.

Meunier C., «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *R.D.P.C.*, 2001, pp. 611 et s.

Roger-France E., «La criminalité informatique», *Actualités de droit pénal*, Bruxelles, Bruylant, 2005, pp. 101-133.

Sieber U., *Legal Aspects of Computer-related Crime in the Information Society – COMCRIME Study – Rapport pour la Commission Européenne*, 1er janvier 1998.

Vandemeulebroeke O., «Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs) – le droit pénal», in *Internet sous le regard du droit*, Bruxelles, Bruylant, 1997, p. 155.

Vandermeersch D., «Le droit pénal et la procédure pénale confrontés à internet», *Internet sous le regard du droit*, Bruxelles, Ed. Jeune Barreau de Bruxelles, 1997, pp. 291 et s.

Van Eecke P., *Criminaliteit in cyberspace : misdrijven, hun opsporing en vervolging op de informatiesnelweg*, Gent, Mys & Breesch, 1997, 121 p.

(331) Loi transposant en droit belge la directive européenne du 11 mars 1996 concernant la protection juridique des bases de données, *M.B.*, 14 novembre 1998.